

Bounded Model Checking of an MITL Fragment for Timed Automata

Roland Kindermann, Tommi Junttila and Ilkka Niemelä

Department of Information and Computer Science

Aalto University

P.O.Box 15400, FI-00076 Aalto, Finland

Email: {Roland.Kindermann,Tommi.Junttila,Ilkka.Niemela}@aalto.fi

Abstract—Timed automata (TAs) are a common formalism for modeling timed systems. Bounded model checking (BMC) is a verification method that searches for runs violating a property using a SAT or SMT solver. MITL is a real-time extension of the linear time logic LTL. Originally, MITL was defined for traces of non-overlapping time intervals rather than the “super-dense” time traces allowing for intervals overlapping in single points that are employed by the nowadays common semantics of timed automata. In this paper we extend the semantics of a fragment of MITL to super-dense time traces and devise a bounded model checking encoding for the fragment. We prove correctness and completeness in the sense that using a sufficiently large bound a counter-example to any given non-holding property can be found. We have implemented the proposed bounded model checking approach and experimentally studied the efficiency and scalability of the implementation.

Keywords—timed automaton; metric interval temporal logic; bounded model checking; satisfiability modulo theories

I. INTRODUCTION

Fully-automated verification has many industrial applications. A particularly interesting and challenging setting for the use of verification are systems for which timing aspects are of high importance like safety instrumented systems or communication protocols. In this paper, we study verification in a setting where *both* the *system* and the *specification* contain quantitative timing aspects, allowing not only to specify, e.g., that a certain situation will eventually lead to a reaction but also that the reaction will happen within a certain amount of time. Allowing such timing aspects to be part of both the specification and the system adds an additional challenge.

Timed automata [1] are a widely employed formalism for the representation of finite state systems augmented with real-valued clocks. Timed automata have been studied for two decades and various tools for the verification of timed automata exist. Most existing verification techniques and tools, like the model checker Uppaal [2], however do not support quantitative specifications on the timing of events. We feel that the ability to state, e.g., that a certain condition triggers a reaction within a certain amount of time provides a clear improvement over being able only to specify that a reaction will eventually occur. For specifications, we use the linear time logic MITL_{0,∞} [3], an extension adding lower

and upper time bounds to the popular logic LTL.

Industrial size systems often have a huge discrete state space in addition to the infinite state space of timing-related parts of the system. We feel that fully symbolic verification is a key to tackling large discrete state spaces. We, thus, provide a translation of a pair of a timed automaton representing a system and a MITL_{0,∞} formula into a symbolic transition system that can serve as a foundation for various symbolic verification methods. It is proven that the translated system has a trace if and only if the original timed automaton has a trace satisfying the formula. We, furthermore, demonstrate how to employ the translation for SMT-based bounded model checking using the region-abstraction for timed automata [1]. We show completeness of the approach and prove the applicability of the region abstraction to the transition system. Finally, we evaluate the scalability of the approach and the cost for checking specifications containing timing experimentally.

MITL_{0,∞} is a fragment of the logic MITL [3] for which the question whether or not a given timed automaton has a trace satisfying or violating a given formula is PSPACE complete [3]. Previously, a verification approach for MITL_{0,∞} specifications was introduced in [3] and improved upon in [4]. At this point, however, there are to our best knowledge no implementations or results of experiments using these methods available. Additionally, a major difference between the techniques described in [3], [4] and our approach lies in the precise semantics of timed automata used. While previous approaches use dense-time semantics, we extend MITL_{0,∞} to super-dense time. Although dense and super-dense time semantics of timed automata are often used interchangeably in the literature (and in fact do not differ in any important fashion when, e.g., verifying reachability constraints), we will show that equivalences between MITL_{0,∞} formulas fundamental to the techniques in [3], [4] do not hold anymore when using dense-time semantics.

II. TIMED AUTOMATA

We first give basic definitions for timed automata (see e.g. [1], [5], [6]). For simplicity, we use basic timed automata in the theoretical parts of the paper. However, in practice (and the experimental part of the paper) one usually defines a network of timed automata that can also have (shared and

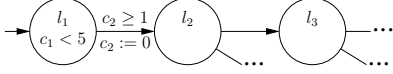


Figure 1. A timed automaton

local) finite domain non-clock variables manipulated on the edges. The symbolic bounded model checking encodings presented later in the paper can be extended to handle both of these features: see, e.g., [7], [8] on how to handle synchronization in a network of timed automata. Alternatively, one can specify timed systems with a symbolic formalism [9].

Let X be a set of real-valued *clock variables*. A *clock valuation* ν is a function $\nu : X \rightarrow \mathbb{R}_{\geq 0}$. For $\delta \in \mathbb{R}_{\geq 0}$ we define the valuation $\nu + \delta$ by $\forall x \in X : (\nu + \delta)(x) = \nu(x) + \delta$. The set of *clock constraints* over X , $\mathcal{C}(X)$, is defined by the grammar $C ::= \text{true} \mid x \bowtie n \mid C \wedge C$ where $x \in X$, $\bowtie \in \{<, \leq, =, \geq, >\}$ and $n \in \mathbb{N}$. A valuation ν satisfies $C \in \mathcal{C}(X)$, denoted by $\nu \models C$, if it evaluates C to true.

A *timed automaton* (TA) is a tuple $\langle L, l_{\text{init}}, X, E, I \rangle$ where

- L is a finite set of *locations*,
- $l_{\text{init}} \in L$ is the *initial location* of the automaton,
- X is a finite set of real-valued *clock variables*,
- $E \subseteq L \times \mathcal{C}(X) \times 2^X \times L$ is a finite set of edges, each edge $\langle l, g, R, l' \rangle \in E$ specifying a *guard* g and a set R of *clocks to be reset*, and
- $I : L \rightarrow \mathcal{C}(X)$ assigns an *invariant* to each location.

As an example, Figure 1 shows a part of a timed automaton with locations l_1, l_2, \dots , and two clocks c_1 and c_2 . The initial location is l_1 , having the invariant $c_1 < 5$. The invariant of the location l_2 is **true**. The edge from l_1 to l_2 has the guard $c_2 \geq 1$ and the reset set $\{c_2\}$. The guard of the edge from l_2 to l_3 is **true** and its reset set is empty.

A *state* of a timed automaton $\mathcal{A} = \langle L, l_{\text{init}}, X, E, I \rangle$ is a pair $\langle l, \nu \rangle$, where $l \in L$ is a location and ν is a clock valuation over X . A state $\langle l, \nu \rangle$ is (i) *initial* if $l = l_{\text{init}}$ and $\nu(x) = 0$ for each $x \in X$, and (ii) *valid* if $\nu \models I(l)$. Let $\langle l, \nu \rangle$ and $\langle l', \nu' \rangle$ be states of \mathcal{A} . There is a *time elapse step* of $\delta \in \mathbb{R}_{>0}$ time units from $\langle l, \nu \rangle$ to $\langle l', \nu' \rangle$, denoted by $\langle l, \nu \rangle \xrightarrow{\delta} \langle l', \nu' \rangle$, if (i) $l = l'$, (ii) $\nu' = \nu + \delta$, and (iii) $\langle l', \nu' \rangle$ is a valid state. Intuitively, there is a time elapse step from a state to another if the second state can be reached from the first one by letting δ amount of time pass. There is a *discrete step* from $\langle l, \nu \rangle$ to $\langle l', \nu' \rangle$, denoted by $\langle l, \nu \rangle \xrightarrow{0} \langle l', \nu' \rangle$, if there is an edge $\langle l, g, R, l' \rangle \in E$ such that (i) $\nu \models g$, (ii) $\langle l', \nu' \rangle$ is a valid state, and (iii) $\nu'(x) = 0$ for all $x \in R$ and $\nu'(x) = \nu(x)$ for all $x \in X \setminus R$. That is, discrete steps can be used to change the current location as long as the guard and the target location invariant are satisfied. A discrete step resets some clocks and leaves the other's values unchanged, i.e., a discrete step does not take any time.

A *run* of \mathcal{A} is an infinite sequence of states $\pi = \langle l_0, \nu_0 \rangle \xrightarrow{\delta_0} \langle l_1, \nu_1 \rangle \xrightarrow{\delta_1} \dots$, such that (i) $\langle l_0, \nu_0 \rangle$ is valid and

initial, and (ii) $\langle l_i, \nu_i \rangle \xrightarrow{\delta_i} \langle l_{i+1}, \nu_{i+1} \rangle$ with some $\delta_i \in \mathbb{R}$ for each consecutive pair of states. E.g., the automaton in Figure 1 has a run $\langle l_1, (0, 0) \rangle \xrightarrow{3.5} \langle l_1, (3.5, 3.5) \rangle \xrightarrow{0} \langle l_2, (3.5, 0.0) \rangle \xrightarrow{0} \langle l_3, (3.5, 0.0) \rangle \xrightarrow{1.1} \langle l_3, (4.6, 1.1) \rangle \dots$ where each clock valuation $\{c_1 \mapsto v, c_2 \mapsto w\}$ is abbreviated with (v, w) . A run is *non-zeno* if the total amount $\sum_{i=0}^{\infty} \delta_i$ of time passed in the run is infinite. In the rest of the paper, we will only consider non-zeno runs.

Observe that on timed automata runs, the automaton can visit multiple locations without time elapsing in between. For instance, at the time point 3.5 in the run given above, the automaton is after the first time elapse step in location l_1 , then after the first discrete step in location l_2 , and finally after the second discrete step in location l_3 . These kind of “super-dense” runs differ from the dense runs that can be represented with “signals”, i.e. by mapping each time point in $\mathbb{R}_{\geq 0}$ to a single value. As we will see in the next section, considering super-dense timed automata runs complicates model checking as, e.g., we cannot get rid of the timed until operator in the way we would if dense runs were used.

Note that previous papers on timed automata use both dense (e.g. [1]) and super-dense time (e.g. [5]), often without addressing the different semantics. From a practical perspective, super-dense runs appear paradox, as they permit multiple successive events to happen with no time passing in between. An alternative way of interpreting super-dense time, however, is that the amount of time in between events is just too small to be of interest and is, thus, abstracted away. We also take the fact that Uppaal [2], arguably the most successful timed model checker, not only allows for super-dense time traces but actually even makes it possible to *enforce* super-dense behaviors by marking locations as “urgent” or “committed” as a strong indication that there is an interest in super-dense traces in practice.

III. THE LOGIC MITL_{0,∞} FOR SUPER-DENSE TIME

Next, we describe the syntax and semantics of MITL_{0,∞} formulas over “super-dense timed traces” which, as discussed in Sect. III-C, can represent timed automata runs.

A. Syntax and Semantics

Assuming a set AP of atomic propositions, the syntax of MITL_{0,∞} formula follows that in [3], and is defined by the BNF grammar $\phi ::= p \mid \phi \mid \neg \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \mathbf{U}_{\bowtie n}^s \phi \mid \phi \mathbf{R}_{\bowtie n}^s \phi$ where p ranges over AP , n ranges over \mathbb{N} , and \bowtie ranges over $\{<, \leq, \geq, >\}$. Intuitively, a strict timed until formula $\phi \mathbf{U}_{\bowtie n}^s \psi$ states that ϕ holds in all later time points until ψ holds at a time point t satisfying the timing constraint, i.e. $t \bowtie n$. Rational time constraints could be allowed in the temporal operators without influencing the expressivity of the logic (see [3] for MITL on dense traces). We define the usual abbreviations: **true** $\equiv (p \vee \neg p)$, **false** $\equiv \neg \text{true}$, $\mathbf{F}_{\bowtie n}^s \phi \equiv \text{true} \mathbf{U}_{\bowtie n}^s \phi$, and $\mathbf{G}_{\bowtie n}^s \phi \equiv \text{false} \mathbf{R}_{\bowtie n}^s \phi$.

We now define the semantics of $\text{MITL}_{0,\infty}$ over “super-dense” timed traces, and then later show the correspondence of timed automata runs to such traces. A *super-dense timed trace* over a set of atomic propositions AP is an infinite sequence $\sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \dots$, where

- each v_i is a subset of AP ,
- each I_i is either an open interval (T_i, T'_i) or a singleton $[T_i, T_i]$ with $0 \leq T_i < T'_i$ and $T_i, T'_i \in \mathbb{R}_{\geq 0}$,
- $I_0 = [0, 0]$,
- for each $i \in \mathbb{N}$ it holds that (i) $I_i = (T_i, T'_i)$ implies $I_{i+1} = [T'_i, T'_i]$, and (ii) $I_i = [T_i, T_i]$ implies either $I_{i+1} = [T_i, T_i]$ or $I_{i+1} = (T_i, T'_{i+1})$; and
- every $t \in \mathbb{R}_{\geq 0}$ is contained in at least one I_i .

For each trace element $\langle I_i, v_i \rangle$, equivalently written as $\langle I_i \rangle$, the interpretation is that the atomic propositions in v_i hold in all the time points in the interval I_i . As consecutive singletons are allowed, it is possible for an atomic proposition to change its value an arbitrary finite number of times at a given time point. This is required to capture timed automata traces containing two or more successive discrete steps and differentiates super-dense timed traces from dense ones. In the semantics part we could have allowed general intervals; however, our constructions depend on discriminating the end points of left/right-closed intervals and thus we use this normal form already here. A *dense timed trace* is a super-dense timed trace with no consecutive singletons (i.e., every time point $t \in \mathbb{R}_{\geq 0}$ occurs in exactly one I_i).

The set of all *points* in a trace σ is defined by $T(\sigma) = \{(i, t) \mid i \in \mathbb{N}, t \in I_i\}$. Two points, $(i, t), (i', t') \in T(\sigma)$, are ordered with the “earlier” relation \prec defined by $(i, t) \prec (i', t') \Leftrightarrow i < i' \vee (i = i' \wedge t < t')$ and the set of all points later than (i, t) is defined by $T_+(\sigma, (i, t)) := \{(i', t') \in T(\sigma) \mid (i, t) \prec (i', t')\}$.

Given a super-dense timed trace σ over AP , a formula ϕ over AP , and a point (i, t) in σ , we define the satisfies relation $\sigma^{(i, t)} \models \phi$ iteratively as follows:

- $\sigma^{(i, t)} \models p$ iff $p \in v_i$, where p is an atomic proposition.
- $\sigma^{(i, t)} \models \neg \phi$ iff $\sigma^{(i, t)} \not\models \phi$ does not hold.
- $\sigma^{(i, t)} \models (\phi \wedge \psi)$ iff $\sigma^{(i, t)} \models \phi$ and $\sigma^{(i, t)} \models \psi$.
- $\sigma^{(i, t)} \models (\phi \vee \psi)$ iff $\sigma^{(i, t)} \models \phi$ or $\sigma^{(i, t)} \models \psi$.
- $\sigma^{(i, t)} \models (\phi \mathbf{U}_{\bowtie n}^s \psi)$ iff $\exists (i', t') \in T_+(\sigma, (i, t)) : (t' - t \bowtie n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$
- $\sigma^{(i, t)} \models (\phi \mathbf{R}_{\bowtie n}^s \psi)$ iff $\forall (i', t') \in T_+(\sigma, (i, t)) : ((t' - t \bowtie n) \wedge \neg(\sigma^{(i', t')} \models \psi)) \Rightarrow (\exists (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \wedge (\sigma^{(i'', t'')} \models \phi))$

For any formula ϕ , we abbreviate $\sigma^{(0, 0)} \models \phi$ with $\sigma \models \phi$.

Example 1: Consider the super-dense timed trace $\sigma = \langle [0, 0] \rangle \langle (0, 4) \rangle \langle [4, 4] \rangle \langle [4, 4] \rangle \langle \{p\} \rangle \langle \{q\} \rangle \langle \emptyset \rangle \dots$. Now $\sigma \models p \mathbf{U}_{\leq 4}^s q$ as $\sigma^{(3, 4)} \models q$ and $\sigma^{(i, t)} \models p$ for all $0 < i < 3$ and $0 \leq t \leq 4$. As another example, $\sigma \models \mathbf{F}_{\leq 3}^s ((\mathbf{G}_{\leq 1}^s p) \wedge (\mathbf{F}_{< 2}^s q))$ also holds because (i) $\sigma^{(1, t)} \models \mathbf{G}_{\leq 1}^s p$ for all $0 \leq t < 3$, and (ii) $\sigma^{(1, t)} \models \mathbf{F}_{< 2}^s q$ for all $2 < t < 4$.

As illustrated in Ex. 1, neither ϕ nor ψ need to hold in the current point in order to satisfy $\phi \mathbf{U}_{\bowtie n}^s \psi$. Conversely, $\phi \mathbf{U}_{\bowtie n}^s \psi$ with $\bowtie \in \{<, \leq\}$ does not necessarily hold even if ψ holds in the first state: e.g., $\langle [0, 0] \rangle \langle (0, 3) \rangle \dots$ does not satisfy $p \mathbf{U}_{< 2}^s q$. As [3] observes, the reason for this slightly unintuitive semantics is that they allow expressing formulas that would not be expressible if more intuitive semantics where the current point in time is relevant for the timed until operator as well were used. On the other hand, expressing that ϕ holds from the current point in time on until ψ holds can be done using the formula $\psi \vee (\phi \wedge (\phi \mathbf{U}_{\bowtie n}^s \psi))$.

We can define the “untimed versions” of the temporal operators with $\mathbf{F}^s \phi \equiv \mathbf{F}_{\geq 0}^s \phi$, $\mathbf{G}^s \phi \equiv \mathbf{G}_{\geq 0}^s \phi$, $\phi \mathbf{U}^s \psi \equiv \phi \mathbf{U}_{\geq 0}^s \psi$, and $\phi \mathbf{R}^s \psi \equiv \phi \mathbf{R}_{\geq 0}^s \psi$. An easily made misconception is that the time-aspect of a timed trace is irrelevant when evaluating “untimed” operators, i.e., that they could be evaluated on ω -words obtained when removing intervals from a trace; this is not the case. In fact, even when not taking the “only in the future” part of the semantics, illustrated in the previous example, into account, considering the sets of propositions only is not sufficient. As an example, the formula $p \mathbf{U}^s q$ is satisfied on $\langle [0, 0] \rangle \langle (0, 2) \rangle \langle [2, 2] \rangle \dots$ but not on $\langle [0, 0] \rangle \langle (0, 2) \rangle \langle [2, 2] \rangle \langle (2, 3.5) \rangle \dots$. The issue in the second trace is that as the interval on which q holds is an open one, any point in it has a previous point at which only p , but not q , holds. This illustrates that even for the “untimed” versions of the operators, timing is relevant.

Observe that with super-dense timed traces we cannot get rid of the timed until operator $\mathbf{U}_{\bowtie n}^s$ by using the “timed until is redundant” theorem of [4], vital for the transducer construction presented there. That is, $\phi \mathbf{U}_{\bowtie n}^s \psi$ is *not* equivalent to $(\mathbf{G}_{\leq n}^s (\phi \mathbf{U} \psi)) \wedge \mathbf{F}_{\geq n}^s \psi$ in our setting.¹ For example, in the trace $\sigma = \langle [0, 0] \rangle \langle (0, 2) \rangle \langle [2, 2] \rangle \langle [2, 2] \rangle \langle [2, 2] \rangle \dots$ we have $\sigma \models p \mathbf{U}_{\geq 2}^s q$ but $\sigma \not\models (\mathbf{G}_{\leq 2}^s (p \mathbf{U} q)) \wedge \mathbf{F}_{\geq 2}^s q$ as $\sigma^{(4, 2)} \not\models p \mathbf{U} q$. Likewise, the corresponding equivalences used in [3] do not hold when using super-dense time, e.g. $p \mathbf{U}_{\geq 2}^s q$ is *not* equivalent to $\mathbf{G}_{< 2}^s p \wedge \mathbf{G}_{\leq 2}^s (q \vee (p \wedge (p \mathbf{U}^s p)))$ which can be demonstrated by the exact same trace.

Similarly, it is not possible to use the classic LTL equality $\phi \mathbf{R} \psi \equiv (\mathbf{G} \psi) \vee (\psi \mathbf{U} (\phi \wedge \psi))$ to handle timed release operator by means of the other operators in our setting: e.g., when $\sigma = \langle [0, 0] \rangle \langle (0, 2) \rangle \langle [2, 2] \rangle \langle [2, 2] \rangle \langle \{q\} \rangle \dots$ we have $\sigma \models \phi \mathbf{R}_{\leq 3}^s \psi$ but $\sigma \not\models \mathbf{G}_{\leq 3}^s \psi$ and $\sigma \not\models \psi \mathbf{U}_{\leq 3}^s (\phi \wedge \psi)$.

One can verify that the usual dualities hold for the operators: $\neg \neg \phi \equiv \phi$, $\neg(\phi \vee \psi) \equiv (\neg \phi) \wedge (\neg \psi)$, $\neg(\phi \wedge \psi) \equiv (\neg \phi) \vee (\neg \psi)$, $\neg(\phi \mathbf{U}_{\bowtie n}^s \psi) \equiv (\neg \phi) \mathbf{R}_{\bowtie n}^s (\neg \psi)$, and $\neg(\phi \mathbf{R}_{\bowtie n}^s \psi) \equiv (\neg \phi) \mathbf{U}_{\bowtie n}^s (\neg \psi)$. These allow us to transform a formula into *positive normal form* in which negations only appear in front of atomic propositions. From now on, we assume that all formulas are in positive normal form.

¹ Here, \mathbf{U} is the non-strict until operator, i.e. $\phi \mathbf{U} \psi := \psi \vee (\phi \wedge (\phi \mathbf{U}^s \psi))$

B. Trace Refinement and Fineness

To perform model checking of $\text{MITL}_{0,\infty}$ formulas, we do not want the values of sub-formulas to change during open intervals. We next formalize this and show how it can be achieved by means of trace refinement; the definitions and results here are extended from those in Sect. 2 of [3].

A trace σ' is a *refinement* of a trace σ , denoted by $\sigma' \preceq \sigma$, if it can be obtained by replacing each open interval $\langle (T_i, T'_i) \rangle$ in the trace σ with a sequence of intervals $\langle (T_{i,0}, T_{i,1}) \rangle \langle (T_{i,1}, T_{i,2}) \rangle \dots \langle (T_{i,k-1}, T_{i,k}) \rangle$ of $2k-1$ consecutive, non-overlapping intervals with $k \geq 1$, $T_{i,0} = T_i$, and $T_{i,k} = T'_i$. Naturally, if ϕ is a $\text{MITL}_{0,\infty}$ formula and σ' is a refinement of σ , then $\sigma' \models \phi$ iff $\sigma \models \phi$.

Taking an arbitrary trace σ , it may happen that the value of a compound sub-formula changes within an open interval. To capture the desired case when this does not happen, we call σ *fine for a formula ϕ* (or ϕ -fine) if for each sub-formula ψ of ϕ (including ϕ itself), for each interval I_i in σ , and for all $t, t' \in I_i$, it holds that $\sigma^{(i,t)} \models \psi$ iff $\sigma^{(i,t')} \models \psi$.

Example 2: The following super-dense timed trace $\sigma = \langle [0,0] \rangle \langle (0,4.1) \rangle \langle [4.1,4.1] \rangle \langle [4.1,4.1] \rangle \langle [4.1,4.1] \rangle \dots$ is not fine for $\mathbf{G}_{\leq 1}^s p$ as, e.g., (i) $\sigma^{(1,t)} \models \mathbf{G}_{\leq 1}^s p$ for all $0 \leq t < 3.1$ but (ii) $\sigma^{(1,t)} \not\models \mathbf{G}_{\leq 1}^s p$ for all $3.1 \leq t < 4.1$. We can make the beginning of the trace $\mathbf{G}_{\leq 1}^s p$ -fine by refining it to $\langle [0,0] \rangle \langle (0,3.1) \rangle \langle [3.1,3.1] \rangle \langle (3.1,4.1) \rangle \langle [4.1,4.1] \rangle \dots$

By definition, every trace σ is fine for each atomic proposition $p \in AP$. Furthermore, if σ is ϕ -fine and ψ -fine, then it is also fine for $\neg\phi$, $\phi \wedge \psi$, and $\phi \vee \psi$. For temporal operators $\mathbf{U}_{\bowtie n}^s$ and $\mathbf{R}_{\bowtie n}^s$, we have the following lemma stating that their values can change only once during an open interval given the trace is fine for the sub-formulas:

Lemma 1: If a trace σ is fine for ϕ and ψ , $i \in \mathbb{N}$, $t, u \in I_i$, $\triangleleft \in \{<, \leq\}$, and $\triangleright \in \{>, \geq\}$, then

- if $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$ and $u \geq t$, then $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$ and $u \leq t$, then $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$ and $u \leq t$, then $\sigma^{(i,u)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$ and $u \geq t$, then $\sigma^{(i,u)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$.

Thus, if σ is fine for two formulas, it can be made fine for their compound by splitting each open interval at most once.

Lemma 2: Let ϕ be a $\text{MITL}_{0,\infty}$ formula and σ a trace. There is a refinement σ' of σ that is ϕ -fine. Such a refinement can be obtained by splitting each open interval in σ into at most 2^K new open intervals and $2^K - 1$ singletons, where K is the number of timed until and release operators in ϕ .

C. Timed Automata Runs as Super-Dense Timed Traces

We now describe the relationship between timed automata runs and super-dense timed traces. In our theory part, when model checking timed automata with $\text{MITL}_{0,\infty}$, we assume that the atomic propositions only concern locations of the automaton. That is, they are of form “@ l_i ”, where l_i is a location in the automaton. Of course, in the practice when

compositions of timed automata with discrete local variables are handled, the atomic propositions can be more complex. However, we do assume that the atomic propositions do not change their values during the time elapse steps.

Consider a run $\pi = \langle l_0, \nu_0 \rangle \xrightarrow{\delta_0} \langle l_1, \nu_1 \rangle \xrightarrow{\delta_1} \dots$ of a timed automaton \mathcal{A} . For each $\langle l_i, \nu_i \rangle$ in π let $t_i = \sum_{j=0}^{i-1} \delta_j$ be the cumulative time spent in the run before the state, i.e. t_i is “the time when the state occurs in π ”. Thus, at the time point t_i the automaton is in the state $\langle l_i, \nu_i \rangle$ and we shall have $\langle [t_i, t_i] \rangle$ in the corresponding timed trace. The time elapse steps in the run produce the missing open intervals: when $\langle l_i, \nu_i \rangle \xrightarrow{\delta_i} \langle l_{i+1}, \nu_{i+1} \rangle$ with $\delta_i > 0$ (and thus $l_i = l_{i+1}$), then an open interval element $\langle (t_i, t_{i+1}) \rangle$ lies in between $\langle [t_i, t_i] \rangle$ and $\langle [t_{i+1}, t_{i+1}] \rangle$ in the timed trace.

Example 3: The run $\langle l_1, (0,0) \rangle \xrightarrow{3.5} \langle l_1, (3.5, 3.5) \rangle \xrightarrow{0} \langle l_2, (3.5, 0) \rangle \xrightarrow{0} \langle l_3, (3.5, 0) \rangle \xrightarrow{1.1} \langle l_3, (4.6, 1.1) \rangle \dots$ of the automaton in Figure 1 corresponds to the trace $\sigma = \langle [0,0] \rangle \langle (0,3.5) \rangle \langle [3.5,3.5] \rangle \langle [3.5,3.5] \rangle \langle [3.5,3.5] \rangle \langle (3.5,4.6) \rangle \dots$

Recall that we will need to consider certain refinements of timed traces when model checking with $\text{MITL}_{0,\infty}$ formulas. All the refinements of a timed trace produced by a timed automata run can be produced by other runs of the same automaton. That is, considering a trace coming from a run $\pi = \langle l_0, \nu_0 \rangle \xrightarrow{\delta_0} \langle l_1, \nu_1 \rangle \xrightarrow{\delta_1} \dots$ of a timed automaton, each refinement can be obtained by considering the corresponding run π' where each time elapse step $\langle l_i, \nu_i \rangle \xrightarrow{\delta_i} \langle l_{i+1}, \nu_{i+1} \rangle$ in π , with $\delta_i > 0$ and $l_{i+1} = l_i$, is split into a sequence $\langle l_i, \nu_i \rangle \xrightarrow{\delta_{i,1}} \langle l_i, \nu_{i,1} \rangle \xrightarrow{\delta_{i,2}} \dots \xrightarrow{\delta_{i,k}} \langle l_i, \nu_{i,k} \rangle$ of time elapse steps such that $\sum_{1 \leq j \leq k} \delta_{i,j} = \delta_i$ (and thus $\nu_{i,k} = \nu_{i+1}$).

IV. SYMBOLIC ENCODING OF TIMED TRACES

We now describe how to *symbolically* represent systems producing super-dense timed traces. The symbolical representation intended not as a replacement for timed automata but as a foundation for their symbolic verification, i.e. it is intended for use in the “back-end” of the verification tool and not as a modeling language. After the formalism is introduced, it will be shown how timed automata can be represented in this framework. The next section will then address the question of how to encode $\text{MITL}_{0,\infty}$ formulas in this framework so that they are symbolically evaluated. Finally, in Sect. VI it will be demonstrated how finite versions of these encodings can be obtained by using region abstraction, allowing us to perform actual symbolic model checking of $\text{MITL}_{0,\infty}$ formulas on timed automata.

A. Symbolic Transition Systems with Clock-like Variables

In the following, we use standard concepts of propositional and first-order logics, and assume that the formulas are interpreted modulo some background theory such as linear arithmetics (see e.g. [10] and the references therein). Given a set of typed variables, a valuation v over the set is a function

that assigns each variable in the set a value in the domain of the variable. We use $v \models \phi$ to denote that v evaluates a quantifier-free formula ϕ over the set to true.

A *symbolic transition system with clock-like variables*, for brevity simply referred to as a transition system for the remainder of the paper, over a set AP of atomic propositions is a tuple $\langle Z, X, \mathcal{I}, \mathcal{INV}, \mathcal{T}, \mathcal{F}, \widehat{AP} \rangle$, where

- $Z = \{z_1, \dots, z_n\}$ is a set of typed *non-clock variables*, $Z' = \{z'_1, \dots, z'_n\}$ being their *next-state versions*,
- $X = \{x_1, \dots, x_m\}$ is a set of non-negative real-valued *clock variables*, $X' = \{x'_1, \dots, x'_m\}$ again being their *next-state versions*,
- \mathcal{I} is the *initial state formula* over $Z \cup X$,
- \mathcal{INV} is the *state invariant formula* over $Z \cup X$,
- \mathcal{T} is the *transition relation formula* over $Z \cup X \cup \{\delta\} \cup Z' \cup X'$, with a real-valued *duration variable* δ ,
- \mathcal{F} is a finite set of *fairness formulas* over Z , and
- \widehat{AP} associates each atomic proposition $p \in AP$ with a corresponding formula \hat{p} over Z .

To ensure that the clock variables are used properly, we require that all the atoms in all the formulas in the system follow these rules: (i) if a non-clock variable in Z or in Z' occurs in the atom, then none of the variables in $X \cup X' \cup \{\delta\}$ occur in it, and (ii) if a variable in $X \cup X' \cup \{\delta\}$ occurs in it, then it is of the forms $x' = 0$, $x' = x + \delta$, $x \bowtie n$, $x + \delta \bowtie n$, or $\delta \bowtie 0$ where $\bowtie \in \{<, \leq, =, \geq, >\}$, $x, x' \in X$ and $n \in \mathbb{N}$. Furthermore, for all valuations τ over $Z \cup X \cup \{\delta\} \cup Z' \cup X'$ such that $\tau \models \mathcal{T}$, it must hold that $\tau(\delta) \geq 0$ and for each clock $x \in X$ either $\tau(x') = 0$ or $\tau(x') = \tau(x) + \tau(\delta)$.

A *state* of the system now is a valuation s over $Z \cup X$ and a *run* an infinite sequence $s_0 \xrightarrow{\delta_0} s_1 \xrightarrow{\delta_1} s_2 \dots$ such that

- $\delta_0 = 0$ and for all $i \in \mathbb{N}$ we have $\delta_i \geq 0$, $s_i(x) \geq 0$ when $x \in X$, and $\delta_i > 0 \Rightarrow \delta_{i+1} = 0$,
- $s_0 \models \mathcal{I}$ and $s_i \models \mathcal{INV}$ holds for all $i \in \mathbb{N}$,
- for all $i \in \mathbb{N}$ it holds that $\{y \mapsto s_i(y) \mid y \in Z \cup X\} \cup \{\delta \mapsto \delta_i\} \cup \{y' \mapsto s_{i+1}(y') \mid y' \in Z' \cup X'\} \models \mathcal{T}$, and
- for each $f \in \mathcal{F}$, there are infinitely many states s in the run for which $s \models f$ holds.

A run $\tau = s_0 \xrightarrow{\delta_0} s_1 \xrightarrow{\delta_1} s_2 \xrightarrow{\delta_2} \dots$ represents the super-dense timed trace $\text{trace}(\tau) = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \langle I_2, v_2 \rangle \dots$ over AP where for each $i \in \mathbb{N}$,

- $v_i = \{p \in AP \mid s_i \models \hat{p}\}$, and
- letting $t_i = \sum_{j=0}^{i-1} \delta_j$, (i) if $\delta_i = 0$, then $I_i = [t_i, t_i]$, and (ii) if $\delta_i > 0$, then $I_i = (t_i, t_i + \delta_i)$.

The set of all traces of a transition system \mathcal{S} is $\text{traces}(\mathcal{S}) = \{\text{trace}(\tau) \mid \tau \text{ is a run of } \mathcal{S}\}$. The transition system \mathcal{S} is *refinement-admitting* if $\sigma \in \text{traces}(\mathcal{S})$ implies $\sigma' \in \text{traces}(\mathcal{S})$ for all the refinements σ' of σ .

B. Encoding Timed Automata Traces

Recall the correspondence between timed automata runs and traces discussed in Sect. III-C. Given a timed automaton

$\mathcal{A} = \langle L, l_{\text{init}}, X, E, I \rangle$, we can encode it as a transition system $\mathcal{S}_{\mathcal{A}} = \langle Z, X, \mathcal{I}, \mathcal{INV}, \mathcal{T}, \emptyset, \widehat{AP} \rangle$, where²

- $Z = \{at\}$, where at is a variable with the domain L ,
- $\mathcal{I} := (at = l_{\text{init}}) \wedge \bigwedge_{x \in X} (x = 0)$,
- $\mathcal{INV} := \bigwedge_{l \in L} (at = l) \Rightarrow I(l)$
- $\mathcal{T} := ((\delta = 0 \wedge \delta' = 0) \Rightarrow \bigvee_{\langle l, g, r, l' \rangle \in E} at=l \wedge at'=l' \wedge g \wedge (\bigwedge_{x \in R} x' = 0) \wedge (\bigwedge_{x \in X \setminus R} x' = x)) \wedge ((\delta > 0 \vee \delta' > 0) \Rightarrow (at' = at \wedge \bigwedge_{x \in X} x' = x + \delta)) \wedge (\delta = 0 \vee \delta' = 0)$
(Recall that δ special real-valued *duration variable*)
- \widehat{AP} associates each atomic proposition $@l$, where $l \in L$, with the formula $(at = l)$.

Now $\text{traces}(\mathcal{S}_{\mathcal{A}})$ is exactly the set of super-dense timed traces corresponding to the runs of the automaton \mathcal{A} . Every state of $\mathcal{S}_{\mathcal{A}}$ corresponds to a time interval in the timed trace of \mathcal{A} . Thus, there are three types of transitions encoded in \mathcal{T} . Firstly, a singleton-to-singleton transition, corresponding to a discrete transition of \mathcal{A} , occurs when δ and δ' are both zero. Secondly, a singleton-to-open transition occurs when the δ is zero and δ' non-zero. On such a transition, all variables remain unchanged. Hence, the clocks values correspond to the left bound of the interval. Thirdly, on a open-to-singleton transition ($\delta > 0$ and $\delta' = 0$) the clock variables are updated according to the length of the open interval.

Due to the “repetition of time elapse steps” property of timed automata discussed in Sect. III-C, the transition system $\mathcal{S}_{\mathcal{A}}$ is also refinement-admitting.

V. SYMBOLIC ENCODING OF MITL_{0,∞} FORMULAS

Let $\mathcal{S} = \langle Z, X, \mathcal{I}, \mathcal{INV}, \mathcal{T}, \mathcal{F}, \widehat{AP} \rangle$ be a transition system over AP encoding some timed system producing super-dense timed traces. We now augment \mathcal{S} with new variables and constraints so that MITL_{0,∞} formulas over AP are symbolically evaluated in the runs of the transition systems. We say that the resulting transition system $\mathcal{S}_{\phi} = \langle Z \cup Z_{\phi}, X \cup X_{\phi}, \mathcal{I} \wedge \mathcal{I}_{\phi}, \mathcal{INV}, \mathcal{T} \wedge \mathcal{T}_{\phi}, \mathcal{F} \cup \mathcal{F}_{\phi}, \widehat{AP} \rangle$ over AP encodes ϕ if Z_{ϕ} includes a Boolean variable $\llbracket \psi \rrbracket$ for each sub-formula ψ of ϕ (including ϕ itself). Furthermore, we require two conditions on such encodings.

First, we want to make sure that the encoding \mathcal{S}_{ϕ} is *sound* in the following senses:

- all the traces of \mathcal{S} (i.e, projections of runs to the atomic propositions) are preserved: $\text{traces}(\mathcal{S}_{\phi}) = \text{traces}(\mathcal{S})$
- when ϕ holds in a state, then it holds in the corresponding interval: for each run $\tau = s_0 s_1 \dots$ of \mathcal{S}_{ϕ} with $\text{trace}(\tau) = \sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \dots$, and each $i \in \mathbb{N}$, $s_i(\llbracket \phi \rrbracket) = \text{true}$ implies $\forall t \in I_i : \sigma^{(i,t)} \models \phi$.

For fine traces we want to faithfully capture the cases when a formula holds on some interval. To this end, we say that

²Strictly, the atoms $\delta' = 0$ and $\delta' > 0$ are not allowed in \mathcal{T} ; this can be handled by adding new Boolean variables $\underline{\delta=0}$ and $\underline{\delta>0}$ in Z , forcing $\underline{\delta=0} \Rightarrow (\delta = 0)$ and $\underline{\delta>0} \Rightarrow (\delta > 0)$ in \mathcal{T} , and then using $\underline{\delta=0'}$ instead of $\delta' = 0$ and $\underline{\delta>0'}$ instead of $\delta' > 0$ in the rest of \mathcal{T} .

the encoding \mathcal{S}_ϕ is *complete* if for every ϕ -fine trace $\sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \langle I_2, v_2 \rangle \dots$ in $\text{traces}(\mathcal{S})$, there is a run $\tau = s_0 s_1 s_2 \dots$ in \mathcal{S}_ϕ such that $\text{trace}(\tau) = \sigma$ and for all points (i, t) in σ it holds that $\sigma^{(i,t)} \models \phi$ implies $v_i(\llbracket \phi \rrbracket) = \mathbf{true}$.

Therefore, our model checking task “Does a refinement-admitting transition system \mathcal{S} have a run corresponding to a trace σ with $\sigma \models \phi$?” is reduced to the problem of deciding whether \mathcal{S}_ϕ has a run $s_0 s_1 s_2 \dots$ with $s_0(\llbracket \phi \rrbracket) = \mathbf{true}$.

A. Encoding Propositional Subformulas

Let $\mathcal{S} = \langle Z, X, \mathcal{I}, \mathcal{IN}\mathcal{V}, \mathcal{T}, \mathcal{F}, \widehat{AP} \rangle$ be a transition system over AP . For the atomic formulas ϕ of forms p and $\neg p$, it is possible to make a transition system $\mathcal{S}_\phi = \langle Z \cup \{\llbracket p \rrbracket\}, X, \mathcal{I}, \mathcal{IN}\mathcal{V}, \mathcal{T} \wedge \mathcal{T}_\phi, \mathcal{F}, \widehat{AP} \rangle$ encoding ϕ by (i) defining $\mathcal{T}_\phi := (\llbracket \phi \rrbracket \Leftrightarrow \hat{p})$ if $\phi = p$ and (ii) $\mathcal{T}_\phi := (\llbracket \phi \rrbracket \Leftrightarrow \neg \hat{p})$ if $\phi = \neg p$. Similarly, assuming that ϕ is either of form $\alpha \wedge \beta$ or $\alpha \vee \beta$ for some MITL_{0,∞} formulas α and β , and that \mathcal{S} encodes both α and β , we can make a transition system $\mathcal{S}_\phi = \langle Z \cup \{\llbracket p \rrbracket\}, X, \mathcal{I}, \mathcal{IN}\mathcal{V}, \mathcal{T} \wedge \mathcal{T}_\phi, \mathcal{F}, \widehat{AP} \rangle$ encoding ϕ as follows: (i) if $\phi = \alpha \vee \beta$, then $\mathcal{T}_\phi := (\llbracket \phi \rrbracket \Leftrightarrow (\llbracket \alpha \rrbracket \vee \llbracket \beta \rrbracket))$, and, (ii) if $\phi = \alpha \wedge \beta$, then $\mathcal{T}_\phi := (\llbracket \phi \rrbracket \Leftrightarrow (\llbracket \alpha \rrbracket \wedge \llbracket \beta \rrbracket))$.

The lemmas for the soundness and completeness of the encodings are given in Sect. V-C.

B. Encoding MITL_{0,∞} operators

In the following sub-sections, we present encodings for the other MITL_{0,∞} operators. In each encoding, we may introduce some new non-clock and clock variables such as c and *lefto*; these variables are “local” to the encoded subformula ψ and not used elsewhere, we do not subscript them (e.g. c really means c_ψ) for the sake of readability. We also introduce new transition relation constraints (i.e. conjuncts in \mathcal{T}_ψ), initial state constraints and fairness conditions. We will use *open* as a shorthand for $(\delta > 0)$.

1) *Encoding $l \mathbf{U}_{\triangleleft n}^s r$ and $l \mathbf{R}_{\triangleleft n}^s r$ with $\triangleleft \in \{<, \leq\}$* : These operators can be expressed with simpler ones by using the following lemma (proven in the appendix):

Lemma 3: $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$ iff $\sigma^{(i,t)} \models (\mathbf{F}_{\triangleleft n}^s \psi) \wedge (\phi \mathbf{U}^s \psi)$ for all $i \in \mathbb{N}$, $t \in I_i$, $\triangleleft \in \{<, \leq\}$, and $n \in \mathbb{N}$.

Using the $\mathbf{U}_{\triangleleft n}^s / \mathbf{R}_{\triangleleft n}^s$ duality, we can now also express $\phi \mathbf{R}_{\triangleleft n}^s \psi$ as $(\mathbf{G}_{\triangleleft n}^s \psi) \wedge (\phi \mathbf{R}^s \psi)$.

2) *Encoding $l \mathbf{U}^s r$* : We encode “untimed” until formulas $l \mathbf{U}^s r$ essentially like in the traditional LTL case [11] but must consider open intervals and singletons separately.

Assume $l \mathbf{U}^s r$ holds on the current interval. If that interval is open, l and one of the following hold: (i) r holds on the current interval, (ii) r holds on the next interval (which is a singleton), or (iii) l holds on the next interval and $l \mathbf{U}^s r$ is satisfied as well. This is captured by the following constraint:

$$\llbracket l \mathbf{U}^s r \rrbracket \wedge \text{open} \Rightarrow \llbracket l \rrbracket \wedge (\llbracket r \rrbracket \vee \llbracket r \rrbracket' \vee (\llbracket l \rrbracket' \wedge \llbracket l \mathbf{U}^s r \rrbracket')) \quad (1)$$

If, in contrast, the current interval is a singleton, then there are two possibilities: (i) the next interval is a singleton and

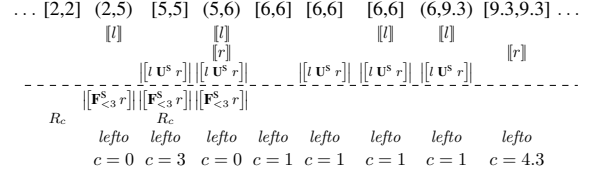


Figure 2. Encoding $l \mathbf{U}^s r$ and $\mathbf{F}_{<3}^s r$

r holds, or (ii) both l and $l \mathbf{U}^s r$ hold on the next interval:

$$\llbracket l \mathbf{U}^s r \rrbracket \wedge \neg \text{open} \Rightarrow (\neg \text{open}' \wedge \llbracket r \rrbracket') \vee (\llbracket l \rrbracket' \wedge \llbracket l \mathbf{U}^s r \rrbracket') \quad (2)$$

Finally, as in the traditional LTL encoding, we must add a fairness condition in order to avoid the case where $\llbracket l \mathbf{U}^s r \rrbracket$ and $\llbracket l \rrbracket$ are **true** on all intervals starting from some point but r does not hold at any future time point, i.e. $\mathcal{F}_{l \mathbf{U}^s r} = \{\neg \llbracket l \mathbf{U}^s r \rrbracket \vee \llbracket r \rrbracket\}$.

Example 4: Figure 2 illustrates an evaluation of the encoding variables on a trace (ignore the text below the dashed line for now). Note that $\llbracket l \mathbf{U}^s r \rrbracket$ is (correctly) evaluated to **true** on the second $[6, 6]$ -interval despite l not holding.

3) *Encoding $\mathbf{F}_{\leq 0}^s r$* : A formula $\mathbf{F}_{\leq 0}^s r$ holding requires a future interval at which r holds and which can be reached without any time passing. Thus, $\mathbf{F}_{\leq 0}^s r$ is satisfied only on a singleton where the next interval is a singleton as well and (i) r or (ii) $\mathbf{F}_{\leq 0}^s r$ holds on the next interval:

$$\llbracket \mathbf{F}_{\leq 0}^s r \rrbracket \Rightarrow \neg \text{open} \wedge \neg \text{open}' \wedge (\llbracket r \rrbracket' \vee \llbracket \mathbf{F}_{\leq 0}^s r \rrbracket') \quad (3)$$

No fairness conditions are needed as the non-zenoness requirement always guarantees a future open interval.

4) *Encoding $\mathbf{F}_{\triangleleft n}^s r$ with $n > 0$* : In the encoding of $\mathbf{F}_{\triangleleft n}^s$, we first add the constraints for \mathbf{U}^s replacing l by **true**.

$$\llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket \wedge \text{open} \Rightarrow \llbracket r \rrbracket \vee \llbracket r \rrbracket' \vee \llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket' \quad (4)$$

$$\llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket \wedge \neg \text{open} \Rightarrow \llbracket r \rrbracket' \vee \llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket' \quad (5)$$

Next, we observe that for encoding timing related aspect, it is sufficient to at any point remember the earliest interval at which $\mathbf{F}_{\triangleleft n}^s r$ holds and after which r has not held yet. If r is encountered in time for the earliest such interval, then interval where r holds is close enough to any later interval where $\llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket$ holds as well. Correspondingly, we use a real-valued (clock-like) auxiliary variable c and a boolean auxiliary variable *lefto* to remember the time passed since and type of the earliest interval on which $\llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket$ held and after which we have not seen $\llbracket r \rrbracket$. The correct values in the first interval are forced by the initial state formula $\mathcal{I}_{\mathbf{F}_{\triangleleft n}^s r} := c = 0 \wedge \neg \text{lefto}$. To update c and *lefto*, we define the shorthand R_c to be **true** when we have not seen $\llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket$ without seeing r afterwards or r holds on an open current or an arbitrary next interval.

$$R_c := (\neg \llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket \vee (\text{open} \wedge \llbracket r \rrbracket) \vee \llbracket r \rrbracket') \wedge \llbracket \mathbf{F}_{\triangleleft n}^s r \rrbracket' \quad (6)$$

We then (i) reset c and $lefto$ on the next interval if R_c holds on the current interval, and (ii) update c and leave $lefto$ unchanged if R_c does not hold.

$$R_c \Rightarrow c' = 0 \wedge (lefto' \Leftrightarrow open') \quad (7)$$

$$\neg R_c \Rightarrow c' = c + \delta \wedge (lefto' \Leftrightarrow lefto) \quad (8)$$

We introduce a shorthand T_c (defined below) such that T_c holds if for each point on the interval where we reset c there is a point on the *next* interval that satisfies the $\triangleleft n$ constraint. We then require that $\llbracket F_{\triangleleft n}^s r \rrbracket$ being **true**, and r being **false** or the current interval being a singleton implies that T_c holds.

$$(\llbracket F_{\triangleleft n}^s r \rrbracket \wedge \neg(\llbracket r \rrbracket \wedge open)) \Rightarrow T_c \quad (9)$$

In the case of $F_{\triangleleft n}^s r$, we define $T_c := c + \delta < n \vee (lefto \wedge c + \delta \leq n)$ and in the case of $F_{\leq n}^s r$ we define $T_c := c + \delta < n \vee ((\neg open' \vee lefto) \wedge c + \delta \leq n)$.

Example 5: An evaluation of the encoding variables is shown (below the dashed line) in Figure 2. Especially, observe that $\llbracket F_{>3}^s r \rrbracket$ is *not* evaluated to true on the interval (6, 9.3) although $F_{>3}^s r$ holds on *some* points in the interval: we are interested in *sound* encodings and $\llbracket F_{>3}^s r \rrbracket$ does not hold on *all* the points in the interval.

5) *Encoding $l U_{\triangleright n}^s r$ with $\triangleright \in \{\geq, >\}$:* To encode $l U_{\triangleright n}^s r$, we define shorthands T_c and \hat{r} . T_c will later be defined so that T_c holds iff for every previous point at which $\llbracket l U_{\triangleright n}^s r \rrbracket$ held there is a point on the current interval that satisfies the $\triangleright n$ timing constraint. We, then, define $\hat{r} := \llbracket r \rrbracket \wedge T_c$. Next, we add a boolean “obligation” variable $oblig$ to remember when we need to see \hat{r} at a future point. Whenever $\llbracket l U_{\triangleright n}^s r \rrbracket$ is **true**, we also require $oblig$ to be **true**.

$$\llbracket l U_{\triangleright n}^s r \rrbracket \Rightarrow oblig \quad (10)$$

In case $n > 0$, we additionally require $oblig$ and l to hold on the next interval.

$$\llbracket l U_{\triangleright n}^s r \rrbracket \Rightarrow (oblig' \wedge l') \quad (11)$$

Next, we add constraints similar to those for the U^s -operator but with $\llbracket l U_{\triangleright n}^s r \rrbracket$ and $\llbracket r \rrbracket$ replaced by $oblig$ and \hat{r} .

$$(oblig \wedge open) \Rightarrow (\llbracket l \rrbracket \wedge (\hat{r} \vee \hat{r}' \vee (\llbracket l \rrbracket' \wedge oblig')) \quad (12)$$

$$(oblig \wedge \neg open) \Rightarrow ((\neg open' \wedge \hat{r}') \vee (\llbracket l \rrbracket' \wedge oblig')) \quad (13)$$

We want to determine whether the $\triangleright n$ constraint holds for *all* previous points at which $\llbracket l U_{\triangleright n}^s r \rrbracket$ holds. We, thus, use a real-valued variable c and a boolean variable $righto$ to measure the time since the most recent corresponding interval. We, thus, reset c to zero and use $righto$ to remember the type of the *current* interval whenever $\llbracket l U_{\triangleright n}^s r \rrbracket$ holds. Otherwise, we update c and $righto$ as before.

$$\llbracket l U_{\triangleright n}^s r \rrbracket \Rightarrow c' = 0 \wedge (righto' \Leftrightarrow open) \quad (14)$$

$$\neg \llbracket l U_{\triangleright n}^s r \rrbracket \Rightarrow c' = c + \delta \wedge (righto' \Leftrightarrow righto) \quad (15)$$

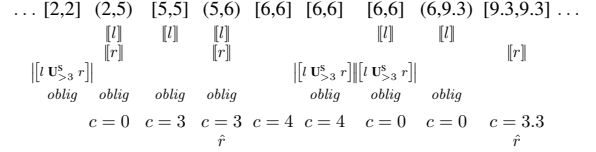


Figure 3. Encoding $l U_{>3}^s r$

Next, in case $l U_{>n}^s r$, we define $T_c := c + \delta > n \vee (righto \wedge c + \delta \geq n)$ and in case $l U_{\geq n}^s r$ we define $T_c := c + \delta > n \vee ((righto \vee \neg open) \wedge c + \delta \geq n)$.

Finally, as for the untimed U^s -operator, we need a fairness condition to prevent a situation where $oblig$ holds globally but r never holds. We define $\mathcal{F}_{l U_{\triangleright n}^s r} := \{\neg oblig \vee \llbracket r \rrbracket\}$. Note that, here, we use $\llbracket r \rrbracket$, not \hat{r} . For instance, when $l U_{\triangleright n}^s r$ and r hold globally, there may never be a point where T_c is **true** and thus \hat{r} always stays **false**.

Example 6: Figure 3 illustrates how the encoding variables of $l U_{>3}^s r$ variables could be evaluated on a trace. Again, $\llbracket l U_{>3}^s r \rrbracket$ is not true on the interval (6, 9.3) because $l U_{>3}^s r$ holds only on some points on it but not on all.

6) *Encoding $l R^s r$:* For encoding $l R^s r$, we use an auxiliary boolean variable $oblig$. Intuitively, $oblig$ being **true** means that before seeing any point at which $\llbracket r \rrbracket$ is **false**, we need to see a point where $\llbracket l \rrbracket$ is **true**.

We require $oblig$ to hold on the current interval when $\llbracket l R^s r \rrbracket$ holds on an open interval and on the next interval when $\llbracket l R^s r \rrbracket$ holds on a singleton.

$$(\llbracket l R^s r \rrbracket \wedge open) \Rightarrow oblig \quad (16)$$

$$(\llbracket l R^s r \rrbracket \wedge \neg open) \Rightarrow oblig' \quad (17)$$

The obligation to see l before $\neg r$ remains active until l holds:

$$oblig \Rightarrow (\llbracket l \rrbracket \vee oblig') \quad (18)$$

As a final constraint, r needs to hold on all intervals where the obligation is **true**, with the exception of open intervals on which l holds, leading to

$$oblig \Rightarrow ((open \wedge \llbracket l \rrbracket) \vee \llbracket r \rrbracket) \quad (19)$$

7) *Encoding $G_{\leq 0}^s r$:* $G_{\leq 0}^s r$ trivially holds when the current or the next interval is open. Furthermore, $G_{\leq 0}^s r$ holds when both current and next interval are singletons and r and $G_{\leq 0}^s r$ hold on the next interval.

$$\llbracket G_{\leq 0}^s r \rrbracket \Rightarrow (open \vee open' \vee (\llbracket r \rrbracket' \wedge \llbracket G_{\leq 0}^s r \rrbracket')) \quad (20)$$

8) *Encoding $G_{\triangleleft n}^s r$ with $n > 0$:* First, we require that r holds on all open intervals on which $\llbracket G_{\triangleleft n}^s r \rrbracket$ holds. Furthermore, we will later define a shorthand T_c to hold whenever there is an interval on which $\llbracket G_{\triangleleft n}^s r \rrbracket$ held sufficiently shortly in the past to still require r to hold, resulting in

$$((\llbracket G_{\triangleleft n}^s r \rrbracket \wedge open) \vee T_c) \Rightarrow \llbracket r \rrbracket \quad (21)$$

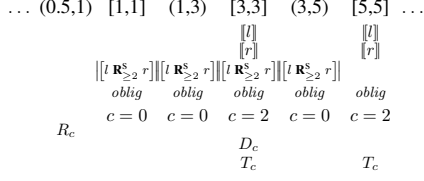


Figure 4. Encoding $l \mathbf{R}_{\geq 2}^s r$.

Like in the $\mathbf{U}_{\triangleright}^s$ encoding, we use a real-valued variable c and a boolean variable *righto* to measure time from the most recent interval at which $\llbracket \mathbf{G}_{\triangleleft n}^s r \rrbracket$ held.

$$\llbracket \mathbf{G}_{\triangleleft n}^s r \rrbracket \Rightarrow c' = 0 \wedge (\text{righto}' \Leftrightarrow \text{open}) \quad (22)$$

$$\neg \llbracket \mathbf{G}_{\triangleleft n}^s r \rrbracket \Rightarrow c' = c + \delta \wedge (\text{righto}' \Leftrightarrow \text{righto}) \quad (23)$$

Now, in the case of $\mathbf{G}_{\leq n}^s$ we define $T_c := c < n$ and for $\mathbf{G}_{\leq n}^s$ we define $T_c := c < n \vee (c \leq n \wedge \neg \text{open} \wedge \neg \text{righto})$

9) *Encoding $l \mathbf{R}_{\triangleright n}^s r$* : For encoding the lower bound until operators, we use a boolean variable *oblig* and the same update rules as for the untimed \mathbf{R}^s operator.

$$(\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket \wedge \text{open}) \Rightarrow \text{oblig} \quad (24)$$

$$(\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket \wedge \neg \text{open}) \Rightarrow \text{oblig}' \quad (25)$$

$$\text{oblig} \Rightarrow (\llbracket l \rrbracket \vee \text{oblig}') \quad (26)$$

We add a modified version of Constraint 18 and use a shorthand T_c (defined later) to identify intervals that contain time points $\triangleright n$ from a point where $\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket$ holds.

$$(\text{oblig} \wedge T_c) \Rightarrow ((\llbracket l \rrbracket \wedge \text{open}) \vee \llbracket r \rrbracket) \quad (27)$$

Next, we add a constraint for intervals of length $> n$. On such an interval, l or r has to hold if $\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket$ holds.

$$(\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket \wedge \delta > n) \Rightarrow (\llbracket l \rrbracket \vee \llbracket r \rrbracket) \quad (28)$$

For encoding $\mathbf{R}_{\triangleright n}^s$, we use an auxiliary real-valued variable c and a boolean variable *lefto* to measure the time passed since the earliest interval at which $\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket$ holds and whose obligation to see l before r is still active. This is, in principle, similar to the $\mathbf{F}_{\triangleleft n}^s$ encoding except for a special case illustrated in Figure 4. Here, on the fourth interval c and *lefto* are needed for two purposes: to measure the time passed since the second interval (which introduced a still open obligation) and to start measuring time since the current interval (which introduces a fresh obligation as $\llbracket l \rrbracket$ holds satisfying the previous obligation). We define a shorthand $D_c := (\neg \text{open} \wedge \text{oblig} \wedge l \wedge \llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket)$ to captures precisely this situation and will later delay resetting c by one step whenever D_c holds. Otherwise, c needs to be reset on the next interval if $\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket$ holds on that interval and (i) if there is an open obligation it is satisfied on the current interval and (ii) the current interval is not a singleton on which $\llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket$ holds, i.e. does not add an obligation to the next interval, i.e. $R_c := \llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket' \wedge (\neg \text{oblig} \vee l) \wedge (\text{open} \vee \neg \llbracket l \mathbf{R}_{\triangleright n}^s r \rrbracket)$.

As said before, we delay resetting c and *lefto* by one interval when D_c holds, i.e. set c to 0 and *lefto* to false.

$$D_c \Rightarrow (c' = 0 \wedge \neg \text{lefto}') \quad (29)$$

When R_c holds, c and *lefto* are reset as for the $\mathbf{F}_{\triangleleft n}^s$ operator and when neither holds we update them as usual:

$$R_c \Rightarrow (c' = 0 \wedge (\text{lefto}' \Leftrightarrow \text{open}')) \quad (30)$$

$$(\neg R_c \wedge \neg D_c) \Rightarrow (c' = c + \delta \wedge (\text{lefto}' \Leftrightarrow \text{lefto})) \quad (31)$$

We set the initial values of c and *lefto* to correspond measuring time from the initial interval, i.e. $\mathcal{I}_{l \mathbf{R}_{\triangleright n}^s r} := c = 0 \wedge \neg \text{lefto}$.

Finally, we define T_c to hold precisely if there is a point on the current interval that is $\triangleright n$ time units away from a point belonging to the interval at which we started measuring time. In the case of $\mathbf{R}_{> n}^s$, we define $T_c := c + \delta > n$ and for $\mathbf{R}_{\geq n}^s$ we define $T_c := c + \delta > n \vee (\neg \text{lefto} \wedge \neg \text{open} \wedge c + \delta \geq n)$.

C. Soundness and Completeness of the Encodings

The encoding just given is sound and complete in the sense defined by the following lemmas which are proven in the appendix.

Lemma 4: The transition system \mathcal{S}_p is a sound encoding for p and $\mathcal{S}_{\neg p}$ is a sound encoding for $\neg p$. If a transition system \mathcal{S} over AP is a sound encoding of α and β , then the transition system $\mathcal{S}_{\text{Op}\alpha}$ over AP is a sound encoding of $\text{Op } \alpha$ for each $\text{Op} \in \{\mathbf{F}_{\leq 0}^s, \mathbf{F}_{< n}^s, \mathbf{F}_{\leq n}^s, \mathbf{G}_{\leq 0}^s, \mathbf{G}_{< n}^s, \mathbf{G}_{\leq n}^s\}$, and $\mathcal{S}_{\alpha \text{Op}\beta}$ is a sound encoding of $\alpha \text{Op } \beta$ for each $\text{Op} \in \{\wedge, \vee, \mathbf{U}^s, \mathbf{U}_{\geq n}^s, \mathbf{U}_{> n}^s, \mathbf{R}^s, \mathbf{R}_{\geq n}^s, \mathbf{R}_{> n}^s\}$.

Lemma 5: The transition system \mathcal{S}_p is a complete encoding for p , $\mathcal{S}_{\neg p}$ is a complete encoding for $\neg p$. If a transition system \mathcal{S} over AP is a complete encoding of α and β , then the transition system $\mathcal{S}_{\text{Op}\alpha}$ over AP is a complete encoding of $\text{Op } \alpha$ for each $\text{Op} \in \{\mathbf{F}_{\leq 0}^s, \mathbf{F}_{< n}^s, \mathbf{F}_{\leq n}^s, \mathbf{G}_{\leq 0}^s, \mathbf{G}_{< n}^s, \mathbf{G}_{\leq n}^s\}$, and $\mathcal{S}_{\alpha \text{Op}\beta}$ is a complete encoding of $\alpha \text{Op } \beta$ for each $\text{Op} \in \{\wedge, \vee, \mathbf{U}^s, \mathbf{U}_{\geq n}^s, \mathbf{U}_{> n}^s, \mathbf{R}^s, \mathbf{R}_{\geq n}^s, \mathbf{R}_{> n}^s\}$.

VI. BOUNDED MODEL CHECKING

Naturally, one cannot directly handle infinite formula representations capturing infinite runs with SMT solvers. Thus in bounded model checking (*BMC*) one considers finite representations, i.e. looping, lasso-shaped paths only. We show that, by using region abstraction [1], we can indeed capture all runs that satisfy a $\text{MITL}_{0,\infty}$ formula with such finite representations. For this we must assume that the domains of all the non-clock variables in Z are finite.

Assume a transition system $\langle Z, X, \mathcal{I}, \mathcal{INV}, \mathcal{T}, \mathcal{F}, \widehat{AP} \rangle$ over a set AP of atomic propositions. For each clock $x \in X$, let m_x be the largest constant n occurring in atoms of forms $x \bowtie n$ and $x + \delta \bowtie n$ in \mathcal{I} , \mathcal{INV} , and \mathcal{T} . Two states, s and t (i.e. valuations over $Z \cup X$ as defined in Sect. IV-A), belong to the same equivalence class called *region*, denoted by $s \approx t$, if (i) $s(z) = t(z)$ for each non-clock variable $z \in Z$, and (ii) for all clocks $x, y \in X$

- 1) either (a) $\lfloor s(x) \rfloor = \lfloor t(x) \rfloor$ or (b) $s(x) > m_x$ and $t(x) > m_x$;
- 2) if $s(x) \leq m_x$, then $\text{fract}(s(x)) = 0$ iff $\text{fract}(t(x)) = 0$, where $\text{fract}(i)$ denotes the fractional part of i ; and
- 3) if $s(x) \leq m_x$ and $s(y) \leq m_y$, then $\text{fract}(s(x)) \leq \text{fract}(s(y))$ iff $\text{fract}(t(x)) \leq \text{fract}(t(y))$.

Next, we will apply the bisimulation property of regions introduced in [1] to transition systems.

Lemma 6: Assume two states, s and t , such that $s \approx t$. It holds that (i) $s \models \mathcal{I}$ iff $t \models \mathcal{I}$, and (ii) $s \models \mathcal{INV}$ iff $t \models \mathcal{INV}$. Furthermore, if there is a $\delta_s \in \mathbb{R}_{\geq 0}$ and a state s' such that $s \cup \{\delta \mapsto \delta_s\} \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\} \models \mathcal{T}$, then there is a $\delta_t \in \mathbb{R}_{\geq 0}$ and a state t' such that $t \cup \{\delta \mapsto \delta_t\} \cup \{y' \mapsto t'(y) \mid y \in X \cup Z\} \models \mathcal{T}$ and $s' \approx t'$. Lemma 6 is proven in the appendix.

When the domains of the non-clock variables are finite, as we have assumed, the set of equivalence classes induced by \approx is finite, too. In this case we can prove, in a similar fashion as the corresponding lemma in [12], that all runs of a transition system also have corresponding runs whose projections on the equivalence classes induced by \approx are lasso-shaped looping runs:

Lemma 7: Let Val be the set of all valuations over Z and Reg the set of clock regions. If the transition system \mathcal{S} has an arbitrary infinite run starting in some state s_0 , then it also has a run $\tau = s_0 \xrightarrow{\delta_0} s_1 \xrightarrow{\delta_1} s_2 \xrightarrow{\delta_2} \dots$ such that for some $i, k \in \mathbb{N}$ with $0 \leq i \leq k \leq (|X| + |\mathcal{F}| + 2) \cdot |Val| \cdot |Reg|$ and for every j with $j \geq i$ we have $s_j \approx s_{j+k-i+1}$.

Intuitively, Lemma 7 states that if \mathcal{S} has a run starting in a given state, then \mathcal{S} has a run starting in the same state that begins to loop *through the same regions* after a finite prefix. E.g., if $i = 7$ and $k = 10$, then $s_7 \approx s_{11} \approx s_{15} \approx s_{19} \dots$ and $s_8 \approx s_{12} \approx s_{16} \approx s_{20} \dots$. In particular, Lemma 7 implies that if we are interested in whether \mathcal{S} has any run at all, it is sufficient to search for runs that are lasso-shaped under the region abstraction. Such runs can be captured with finite bounded model checking encodings. Given a formula ψ over $Z \cup X \cup \{\delta\} \cup Z' \cup X'$ and an index $i \in \mathbb{N}$, let $\psi^{[i]}$ be the formula over $\{y^{[i]} \mid y \in Z \cup X \cup \{\delta\}\} \cup \{y^{[i+1]} \mid y \in Z \cup X\}$ obtained by replacing each variable $y \in Z \cup X \cup \{\delta\}$ with the variable $y^{[i]}$ and each $y' \in Z' \cup X'$ with the variable $y^{[i+1]}$. E.g., $((x' = x + \delta) \wedge \neg p)^{[3]}$ is $(x^{[4]} = x^{[3]} + \delta^{[3]}) \wedge \neg p^{[3]}$. Now the bounded model checking encoding for bound k is:

$$\begin{aligned} \llbracket \mathcal{S}, k \rrbracket := & \delta^{[0]} = 0 \wedge \mathcal{I}^{[0]} \wedge \bigwedge_{0 \leq j \leq k} \mathcal{INV}^{[j]} \wedge \\ & \bigwedge_{0 \leq j < k} \mathcal{T}^{[j]} \wedge \bigwedge_{1 \leq j \leq k} (\text{loop}^{[j]} \Rightarrow E_{j,k}) \wedge \\ & \bigwedge_{0 \leq j < k} (\delta^{[j]} > 0 \Rightarrow \delta^{[j+1]} = 0) \wedge \\ & \text{Fair}_k \wedge \text{NonZeno}_k \wedge \bigvee_{1 \leq j \leq k} \text{loop}^{[j]} \end{aligned}$$

where (i) $E_{j,k}$ is a formula evaluating to true if state $j-1$ and state k (i.e. the valuations of the variables with superscripts $j-1$ and k , respectively) are in the same region (see [12] for different ways to implement this), and (ii) Fair_k and

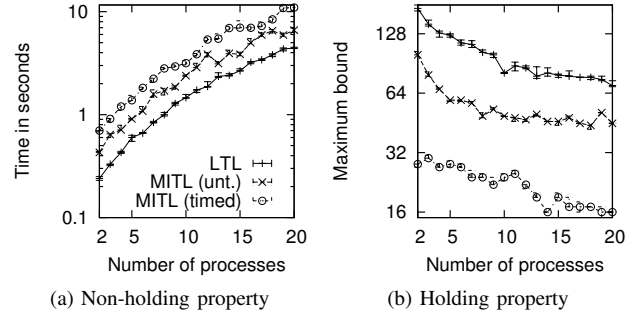


Figure 5. Experimental results

NonZeno_k are constraints forcing that the fairness formulas are holding in the loop and that sufficiently much time passes in the loop to unroll it to a non-zeno run (again, see [12]). Intuitively, the conjuncts of $\llbracket \mathcal{S}, k \rrbracket$ encode the following: (a) the first interval is a singleton and satisfies the initial constraint, (b) all intervals satisfy the invariant and all pairs of successive states the transition relation, (c) if some $\text{loop}^{[j]}$ holds then state $j-1$ and state k are in the same region, (d) there are no two successive open intervals, (e) the fairness formulas are satisfied within the looping part of the trace, (f) the trace is non-zeno and (g) at least one $\text{loop}^{[j]}$ is true, meaning that the trace is “looping under region abstraction”.

Now, if we wish to find out whether a transition system \mathcal{S} has a run corresponding to a trace σ such that $\sigma \models \phi$ for a $\text{MITL}_{0,\infty}$ formula ϕ , we can check whether $\llbracket \mathcal{S}, k \rrbracket \wedge \llbracket \phi \rrbracket^{[0]}$ is satisfiable for some $0 < k \leq (|X| + |\mathcal{F}| + 2) \cdot |Val| \cdot |Reg|$. This upper bound is very large and, in practice, much lower bounds are often used (and sufficient for finding traces). Then, however, the possibility remains that a trace exists despite none being found with the bound used.

VII. EXPERIMENTAL EVALUATION

We have studied the feasibility of the BMC encoding developed in this paper experimentally. We have devised a straightforward implementation of the approach following the encoding scheme given in Sect. IV and V. With experiments on a class of models we (i) show that it is possible to develop relatively efficient implementations of the approach, (ii) demonstrate that the approach scales reasonably and (iii) are able to estimate the cost of timing by comparing the verification of properties using timed operators both to verifying $\text{MITL}_{0,\infty}$ properties that do not use timing constraints and region-based LTL BMC [12], [13].

As a model for the experimentation we used the Fischer mutual exclusion protocol with two to 20 agents. This protocol is commonly used for the evaluation of timed verification approaches. The encoding used for the experiments is based on a model that comes with the model checker Uppaal [2] which also uses super-dense time. We checked one property

that holds (“requesting state leads to waiting state eventually”) and one that does not (“there is no trace visiting the critical section and the non-critical section infinitely often”).³ Each property was checked in three variants: as an LTL property using the approach from [12], as the corresponding MITL property (only untimed operators) and with timing constraints added. Both MITL BMC and LTL BMC were used in an incremental fashion, i.e. bounds are increased starting with bound one until a counter-example is found and constraints are shared by successive SMT solver calls where possible. All experiments were run under Linux on Intel Xeon X5650 CPUs limiting memory to 4 GB and CPU time to 20 minutes. As an SMT solver, Yices [14] version 1.0.37 was used. All plots report minimum, maximum and median over 11 executions. The implementation and the benchmark used are available on the first author’s website.

Figure 5a shows the time needed for finding a counter-example to the non-holding property. No timeouts were encountered, even when using the timed MITL properties. Figure 5b shows the maximum bound reached within 20 minutes when checking the holding property. The bounds reached for the timed property are significantly lower than the bounds reached for the LTL property with the untimed MITL BMC bounds lying between. While there is both a cost for using the MITL framework for an untimed property and an additional cost for adding timing constraints, checking timed constraints using MITL BMC is certainly feasible. The performance could be further improved using well-known optimization techniques e.g. by adding the possibility for finite counter-examples [11], a technique used in the LTL BMC implementation used for the experiments. When verifying properties without timing constraints, using LTL BMC, however, is advisable not only because of the better performance but also because a lower bound is needed to find a trace as open intervals are irrelevant for LTL formulas.

VIII. CONCLUSIONS

In this paper, we extend the linear time logic $\text{MITL}_{0,\infty}$ to super-dense time semantics. We devise a method to encode both a timed automaton and a $\text{MITL}_{0,\infty}$ formula as a symbolic transition system. The encoding provides a foundation for different kinds of fully symbolic verification methods. Soundness and completeness of the encoding are proven in the appendix. Furthermore, we demonstrate how the encoding can be employed for bounded model checking (BMC) using the well-known region abstraction. We have implemented the approach. An experimental evaluation of the BMC approach indicated that a reasonably efficient implementation is feasible.

ACKNOWLEDGEMENTS

This work has been financially supported by the Academy of Finland under project 128050 and under the Finnish

Centre of Excellence in Computational Inference (COIN).

REFERENCES

- [1] R. Alur and D. L. Dill, “A theory of timed automata,” *Theoretical Computer Science*, vol. 126, no. 2, pp. 183–235, 1994.
- [2] G. Behrmann, A. David, and K. G. Larsen, “A tutorial on UPPAAL,” in *Proc. FM-RT 2004*, ser. LNCS, vol. 3185. Springer, September 2004, pp. 200–236.
- [3] R. Alur, T. Feder, and T. A. Henzinger, “The benefits of relaxing punctuality,” *Journal of the ACM*, vol. 43, no. 1, pp. 116–146, 1996.
- [4] O. Maler, D. Nickovic, and A. Pnueli, “From MITL to timed automata,” in *FORMATS*, ser. LNCS, vol. 4202. Springer, 2006, pp. 274–289.
- [5] R. Alur, “Timed automata,” in *Proc. CAV 1999*, ser. LNCS, vol. 1633. Springer, 1999, pp. 8–22.
- [6] J. Bengtsson and W. Yi, “Timed automata: Semantics, algorithms and tools,” in *Lectures on Concurrency and Petri Nets*, ser. LNCS, vol. 3098. Springer, 2004, pp. 87–124.
- [7] M. Sorea, “Bounded model checking for timed automata,” *Elect. Notes Theor. Comp. Sci.*, vol. 68, no. 5, pp. 116–134, 2002.
- [8] G. Audemard, A. Cimatti, A. Kornilowicz, and R. Sebastiani, “Bounded model checking for timed systems,” in *Proc. FORTE 2002*, ser. LNCS, vol. 2529. Springer, 2002, pp. 243–259.
- [9] R. Kindermann, T. Junttila, and I. Niemelä, “Modeling for symbolic analysis of safety instrumented systems with clocks,” in *Proc. ACS D 2011*. IEEE, 2011, pp. 185–194.
- [10] C. Barrett, R. Sebastiani, S. A. Seshia, and C. Tinelli, “Satisfiability modulo theories,” in *Handbook of Satisfiability*. IOS Press, 2009, pp. 825–885.
- [11] A. Biere, K. Heljanko, T. Junttila, T. Latvala, and V. Schuppan, “Linear encodings of bounded LTL model checking,” *Logical Methods in Computer Science*, vol. 2, no. 5:5, pp. 1–64, 2006.
- [12] R. Kindermann, T. Junttila, and I. Niemelä, “Beyond lassos: Complete SMT-based bounded model checking for timed automata,” in *Proc. FORTE 2012*, ser. LNCS, vol. 7273. Springer, 2012, pp. 84–100.
- [13] A. Biere, A. Cimatti, E. M. Clarke, and Y. Zhu, “Symbolic model checking without BDDs,” in *Proc. TACAS 1999*, ser. LNCS, vol. 1579. Springer, 1999, pp. 193–207.
- [14] B. Dutertre and L. M. de Moura, “A fast linear-arithmetic solver for DPLL(T),” in *Proc. CAV 2006*, ser. LNCS, vol. 4144. Springer, 2006, pp. 81–94.

³Here, we search for counter-examples, i.e. encode $\neg\phi$ instead of ϕ .

APPENDIX

A. Duality of until and release operators

Lemma 8: For any trace $\sigma = \langle I_0, v_0 \rangle, \langle I_1, v_1 \rangle, \dots$ over AP , $\text{MITL}_{0,\infty}$ formulas ϕ and ψ over AP , $i \in \mathbb{N}$, $t \in I_i$ it holds that $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\bowtie n}^s \psi)$ iff $\sigma^{(i,t)} \models \neg(\neg\phi \mathbf{R}_{\bowtie n}^s \neg\psi)$

Proof: $\sigma^{(i,t)} \models \neg(\neg\phi \mathbf{R}_{\bowtie n}^s \neg\psi)$ if and only if (by definition)

$$\neg \forall (i', t') \in T_+(\sigma, (i, t)) : ((t' - t \bowtie n) \wedge \neg(\sigma^{(i', t')} \models \neg\psi)) \Rightarrow (\exists (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \wedge (\sigma^{(i'', t'')} \models \neg\phi))$$

if and only if (pushing negations inside)

$$\exists (i', t') \in T_+(\sigma, (i, t)) : ((t' - t \bowtie n) \wedge \neg(\sigma^{(i', t')} \models \neg\psi)) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \Rightarrow \neg(\sigma^{(i'', t'')} \models \neg\phi))$$

if and only if (replacing $\neg(\sigma^{(i', t')} \models \neg\cdot)$ by $(\sigma^{(i', t')} \models \cdot)$)

$$\exists (i', t') \in T_+(\sigma, (i, t)) : (t' - t \bowtie n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$$

if and only if (by definition) $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\bowtie n}^s \psi)$. \blacksquare

Lemma 9: For any trace $\sigma = \langle I_0, v_0 \rangle, \langle I_1, v_1 \rangle, \dots$ over AP , $\text{MITL}_{0,\infty}$ formulas ϕ and ψ over AP , $i \in \mathbb{N}$, $t \in I_i$ it holds that $\sigma^{(i,t)} \models (\phi \mathbf{R}_{\bowtie n}^s \psi)$ iff $\sigma^{(i,t)} \models \neg(\neg\phi \mathbf{U}_{\bowtie n}^s \neg\psi)$

Proof: $\sigma^{(i,t)} \models \neg(\neg\phi \mathbf{U}_{\bowtie n}^s \neg\psi)$ iff (by Lemma 8) $\sigma^{(i,t)} \models \neg(\neg(\neg\phi \mathbf{R}_{\bowtie n}^s \neg\neg\psi))$ iff (double negations) $\sigma^{(i,t)} \models (\phi \mathbf{R}_{\bowtie n}^s \psi)$. \blacksquare

B. Proof of Lemma 1

Lemma 1: If a trace σ is fine for ϕ and ψ , $i \in \mathbb{N}$, $t, u \in I_i$, $\triangleleft \in \{<, \leq\}$, and $\triangleright \in \{\geq, >\}$, then

- if $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$ and $u \geq t$, then $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$ and $u \leq t$, then $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$ and $u \leq t$, then $\sigma^{(i,u)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$;
- if $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$ and $u \geq t$, then $\sigma^{(i,u)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$.

Proof: If I_i is a singleton, then the lemma holds trivially. Thus, assume that I_i is an open interval. We have the following four cases.

- Assume that $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$. Thus there exists a $(i', t') \in T_+(\sigma, (i, t))$ such that $(t' - t \triangleleft n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$. Let $u \geq t$ with $u \in I_i$. Now $T_+(\sigma, (i, u)) \subseteq T_+(\sigma, (i, t))$.
If $i' > i$ or $i' = i \wedge u < t'$, then $(t' - u \triangleleft n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, u)), (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$, implying $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$ irrespective whether σ is fine for ϕ and ψ or not.
If $i' = i$ and $u \geq t'$, then there is a $u' > u$ with $u' \in I_i$ and $u' - u \triangleleft n$ as I_i is an open interval. As σ is fine for ψ and $\sigma^{(i, t')} \models \psi$, it holds that $\sigma^{(i, u')} \models \psi$ as well. As $\forall (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i, t') \Rightarrow (\sigma^{(i'', t'')} \models \phi)$, there is at least one $t < t'' < t'$, and σ is fine for ϕ , we have $\forall (i'', u'') \in T_+(\sigma, (i, u)), (i'', u'') \prec (i, u') \Rightarrow (\sigma^{(i'', u'')} \models \phi)$. Therefore, $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$.

- Assume that $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$. Thus there exists a $(i', t') \in T_+(\sigma, (i, t))$ such that $(t' - t \triangleright n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$. Let $u \leq t$ with $u \in I_i$. Thus $t' - u \triangleright n$. Because (i) $\forall (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi)$, (ii) there is at least one $t < t'' < t'$ with $t'' \in I_i$ as I_i is open, and (iii) σ is fine for ϕ , we have $\forall (i'', t'') \in T_+(\sigma, (i, u)), (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi)$. Therefore, $\sigma^{(i,u)} \models \phi \mathbf{U}_{\triangleright n}^s \psi$.

- Assume that $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$. Thus $\forall (i', t') \in T_+(\sigma, (i, t)), ((t' - t \triangleleft n) \wedge \neg(\sigma^{(i', t')} \models \psi)) \Rightarrow (\exists (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i', t') \wedge (\sigma^{(i'', t'')} \models \phi))$. Let $u \leq t$ with $u \in I_i$.

Suppose that $(u' - t' \triangleleft n) \wedge \neg(\sigma^{(j', u')} \models \psi)$ for some $(j', u') \in T_+(\sigma, (i, u))$. If $(i, t) \prec (j', u')$, then $\exists (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (j', u') \wedge (\sigma^{(i'', t'')} \models \phi)$. On the other hand, if $(j', u') = (i, t)$ or $(j', u') \prec (i, t)$, then $j' = i$, $\neg(\sigma^{(i, v)} \models \psi)$ for all $v \in I_i$ as σ is fine for ψ , there is a $(i, t'') \in T_+(\sigma, (i, t)), (i, t) \prec (i, t'') \wedge (\sigma^{(i, t'')} \models \phi)$ as I_i is open, $\sigma^{(i, v)} \models \phi$ for all $v \in I_i$ as σ is fine for ϕ , and $\sigma^{(i, u)} \models \phi \mathbf{R}_{\triangleleft n}^s \psi$.

- Assume that $\sigma^{(i,t)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$. Thus $\forall (i', t') \in T_+(\sigma, (i, t)), ((t' - t \triangleright n) \wedge \neg(\sigma^{(i', t')} \models \psi)) \Rightarrow (\exists (i'', t'') \in T_+(\sigma, (i, t)), (i'', t'') \prec (i', t') \wedge (\sigma^{(i'', t'')} \models \phi))$. Let $u \geq t$ with $u \in I_i$. Suppose that $(u' - u \triangleright n) \wedge \neg(\sigma^{(j', u')} \models \psi)$ for some $(j', u') \in T_+(\sigma, (i, u))$. As $u' - t \triangleright n$, there exists a $(i'', t'') \in T_+(\sigma, (i, t))$ such that $(i'', t'') \prec (i', t') \wedge (\sigma^{(i'', t'')} \models \phi)$. If $(j', u') \prec (i'', t'')$, we are done. On the other hand, if $(i'', t'') = (j', u')$ or $(i'', t'') \prec (j', u')$, then $\sigma^{(i, v)} \models \phi$ for all $v \in I_i$ as σ is fine for ϕ , there exists a (i, j'') such that $(i, j) \prec (i, j'') \prec (j', u')$ as I_i is open, and thus $\sigma^{(i, u)} \models \phi \mathbf{R}_{\triangleright n}^s \psi$. \blacksquare

C. Proof of Lemma 2

Lemma 2: Let ϕ be a $\text{MITL}_{0,\infty}$ formula and σ a trace. There is a refinement σ' of σ that is ϕ -fine. Such a refinement can be obtained by splitting each open interval in σ into at most 2^K new open intervals and $2^K - 1$ singletons, where K is the number of timed until and release operators in ϕ .

Proof: Let $[\phi_1, \dots, \phi_n]$ be a list containing all the sub-formulas of ϕ so that the sub-formulas of a sub-formula ϕ_i are listed before ϕ_i . Thus ϕ_1 is an atomic proposition and $\phi_n = \phi$.

We now construct a trace σ_i for each $1 \leq i \leq n$ such that σ_i is fine for all sub-formulas ϕ_j with $1 \leq j \leq i$.

If ϕ_i is an atomic proposition or of forms $\neg\phi_j$, $\phi_j \wedge \phi_k$, or $\phi_j \vee \phi_k$ with $j, k < i$, then $\sigma_i = \sigma_{i-1}$ is fine for ϕ_i as well.

If ϕ_i is an until or release formula of forms $\phi_j \mathbf{U}_{\bowtie n}^s \phi_k$ or $\phi_j \mathbf{R}_{\bowtie n}^s \phi_k$, then by (i) recalling that σ_{i-1} is fine for ϕ_j

and ϕ_k (ii) applying Lemma 1, we obtain a ϕ_i -fine trace σ_i by splitting each open interval in σ_{i-1} into at most two new open intervals and one singleton interval. ■

D. Proof of Lemma 3

Lemma 3: $\sigma^{(i,t)} \models \phi \mathbf{U}_{\triangleleft n}^s \psi$ iff $\sigma^{(i,t)} \models (\mathbf{F}_{\triangleleft n}^s \psi) \wedge (\phi \mathbf{U}^s \psi)$ for all $i \in \mathbb{N}$, $t \in I_i$, $\triangleleft \in \{<, \leq\}$, and $n \in \mathbb{N}$.

Proof: Recall that $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\triangleleft n}^s \psi)$ iff $\exists (i', t') \in T_+(\sigma, (i, t)) : (t' - t \triangleleft n) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$.

- The “ \Rightarrow ” part.

As is easy to see from the semantics, $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\triangleleft n}^s \psi)$ implies both (i) $\sigma^{(i,t)} \models (\phi \mathbf{U}^s \psi)$ and (ii) $\sigma^{(i,t)} \models (\mathbf{true} \mathbf{U}_{\triangleleft n}^s \psi)$ corresponding to $\sigma^{(i,t)} \models \mathbf{F}_{\triangleleft n}^s \psi$.

- The “ \Leftarrow ” part.

By the semantics, if $\sigma^{(i,t)} \models (\phi \mathbf{U}^s \psi)$ we can pick a $(i', t') \in T_+(\sigma, (i, t))$ such that $(t' - t \geq 0) \wedge (\sigma^{(i', t')} \models \psi) \wedge (\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (i', t') \Rightarrow (\sigma^{(i'', t'')} \models \phi))$. We have two cases now:

- If $t' - t \triangleleft n$, then we immediately have $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\triangleleft n}^s \psi)$.
- Otherwise, $\sigma^{(i,t)} \models \mathbf{F}_{\triangleleft n}^s \psi$ allows us to pick $(j', u') \in T_+(\sigma, (i, t))$ such that $(u' - t \triangleleft n) \wedge (\sigma^{(j', u')} \models \psi)$. As $u' - t \triangleleft n$, we know that $(j', u') \prec (i', t')$, which in turn implies that $\forall (i'', t'') \in T_+(\sigma, (i, t)) : (i'', t'') \prec (j', u') \Rightarrow (\sigma^{(i'', t'')} \models \phi)$. Thus we obtain $\sigma^{(i,t)} \models (\phi \mathbf{U}_{\triangleleft n}^s \psi)$. ■

E. Soundness proofs

Lemma 4: The transition system \mathcal{S}_p is a sound encoding for p and $\mathcal{S}_{\neg p}$ is a sound encoding for $\neg p$. If a transition system \mathcal{S} over AP is a sound encoding of α and β , then the transition system $\mathcal{S}_{\mathbf{Op}\alpha}$ over AP is a sound encoding of $\mathbf{Op} \alpha$ for each $\mathbf{Op} \in \{\mathbf{F}_{\leq 0}^s, \mathbf{F}_{< n}^s, \mathbf{F}_{\leq n}^s, \mathbf{G}_{\leq 0}^s, \mathbf{G}_{< n}^s, \mathbf{G}_{\leq n}^s\}$, and $\mathcal{S}_{\alpha \mathbf{Op} \beta}$ is a sound encoding of $\alpha \mathbf{Op} \beta$ for each $\mathbf{Op} \in \{\wedge, \vee, \mathbf{U}^s, \mathbf{U}_{\geq n}^s, \mathbf{U}_{> n}^s, \mathbf{R}^s, \mathbf{R}_{\geq n}^s, \mathbf{R}_{> n}^s\}$.

Recall, that we call an encoding \mathcal{S}_ϕ is sound if the following are satisfied:

- all the traces of \mathcal{S} (i.e., projections of runs to the atomic propositions) are preserved: $\text{traces}(\mathcal{S}_\phi) = \text{traces}(\mathcal{S})$
- when ϕ holds in a state, then it holds in the corresponding interval: for each run $\tau = s_0 s_1 \dots$ of \mathcal{S}_ϕ with $\text{trace}(\tau) = \sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \dots$, and each $i \in \mathbb{N}$, $s_i(\llbracket \phi \rrbracket) = \mathbf{true}$ implies $\forall t \in I_i : \sigma^{(i,t)} \models \phi$.

We will now prove Lemma 4 separately for each operator. Note, that as we assumed \mathcal{S} to be sound for α and β , we know that any point on a run where $\llbracket \alpha \rrbracket$ holds satisfies α and any point where $\llbracket \beta \rrbracket$ holds satisfies β , which will be used in the proofs without being mentioned explicitly every single time.

Proof: For $\mathbf{Op} \in \{\wedge, \vee\}$. Clearly, all runs are preserved. Also, by the constraint that $\llbracket \alpha \mathbf{Op} \beta \rrbracket \Leftrightarrow \llbracket \alpha \rrbracket \mathbf{Op} \llbracket \beta \rrbracket$, it immediately follows that for any $i \in \mathbb{N}$ we have $\forall t \in I_i : s_i(\llbracket \alpha \mathbf{Op} \beta \rrbracket) \Rightarrow (\sigma^{(i,t)} \models \alpha \mathbf{Op} \beta)$. ■

Proof: For $\mathbf{Op} = \mathbf{U}^s$. Clearly, all the traces are preserved in $\mathcal{S}_{\alpha \mathbf{U}^s \beta}$ as setting $\llbracket \alpha \mathbf{U}^s \beta \rrbracket$ to **false** leads to both constraints being satisfied regardless of the trace.

Now take a $\mathcal{S}_{\alpha \mathbf{U}^s \beta}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.

If I_i is open, then by Constraint 1 we know that $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$. Furthermore, there are three possibilities (multiple of which may be applicable):

- 1) $s_i(\llbracket \beta \rrbracket) = \mathbf{true}$. In this case we can pick any future time point on the open interval i and demonstrate that β holds there and α holds up to that point, meaning that $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.
- 2) $s_{i+1}(\llbracket \beta \rrbracket) = \mathbf{true}$. As I_i is open, we know that I_{i+1} is a singleton. Furthermore, as $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$ we know that α holds up to the single time point constituting I_{i+1} . Hence, $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.
- 3) $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$ and $s_i(\llbracket \beta \rrbracket) = s_{i+1}(\llbracket \beta \rrbracket) = \mathbf{false}$. By Constraint 1, then $s_{i+1}(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$. By the fairness constraint $\mathcal{F}_{\alpha \mathbf{U}^s \beta}$ we know that there is a future interval on which either $\llbracket \beta \rrbracket$ holds or $\llbracket \alpha \mathbf{U}^s \beta \rrbracket$ does not hold. Pick $j > i + 1$ as small as possible, such that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ or $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{false}$. Now $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \dots = s_{j-1}(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ and $s_i(\llbracket \beta \rrbracket) = \dots = s_{j-1}(\llbracket \beta \rrbracket) = \mathbf{false}$. Note that the only way to satisfy Constraints 1 and 2 on intervals $i, \dots, j - 2$ now is by $\llbracket \alpha \rrbracket'$ holding on those intervals, meaning that $s_{i+1}(\llbracket \alpha \rrbracket) = \dots = s_{j-1}(\llbracket \alpha \rrbracket) = \mathbf{true}$.
Now

- If I_{j-1} is open, then by Constraint 1 we know that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ or $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$. As we picked j so that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ or $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{false}$, we know that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ (meaning that β holds at interval j) in either case. Furthermore, as I_{j-1} is open we know that I_j is a singleton, implying that $\llbracket \alpha \rrbracket$ (and thus α) holds anywhere in between (i, t) and I_j . Thus, $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.
- If I_{j-1} is a singleton, then by Constraint 2 we know that either $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ and I_j is a singleton or $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = s_j(\llbracket \alpha \rrbracket) = \mathbf{true}$. Again, by the choice of j we know that $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ implies that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$. Thus, there is in either case a time point in interval j at which $\llbracket \beta \rrbracket$ (and thus β) holds such that $\llbracket \alpha \rrbracket$ (and thus α) holds anywhere in between (i, t) and that time point. Hence, $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.

If, in contrast, I_i is a singleton, then by Constraint 2 there are two possibilities:

- 1) I_{i+1} is a singleton and $s_{i+1}(\llbracket \beta \rrbracket) = \mathbf{true}$. In this case, trivially $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.
- 2) $s_{i+1}(\llbracket \alpha \rrbracket) = s_{i+1}(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$. If additionally $s_{i+1}(\llbracket \beta \rrbracket) = \mathbf{true}$, then $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$ indiscriminately of whether I_{i+1} is a singleton or an open interval. If, in contrast, $s_{i+1}(\llbracket \beta \rrbracket) = \mathbf{false}$, then we can, again, pick $j > i + 1$ as small as possible, such that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ or $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{false}$. By proceeding precisely in the same way as in the Case 3 for open I_i , we can again deduce that $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$.

Thus, $\sigma^{(i,t)} \models \alpha \mathbf{U}^s \beta$ holds in each of the described cases. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{\leq 0}^s$.

Again, the “preservation of traces” property follows from the fact that the constraint is trivially satisfied globally when $\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket$ is set to **false** globally.

Now take a $\mathcal{SF}_{\leq 0}^s \alpha$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \mathbf{F}_{\leq 0}^s \alpha$.

By Constraint 3, we now know that I_i and I_{i+1} are both singletons. This, in particular, means that $I_{i+1} = [t, t]$. Furthermore, by Constraint 3 one of the following holds:

- $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$. In this case, $\sigma^{(i,t)} \models \mathbf{F}_{\leq 0}^s \alpha$ trivially.
- $s_{i+1}(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. In this case, I_{i+2} is a singleton as well and again $s_{i+2}(\llbracket \alpha \rrbracket) = \mathbf{true}$ or $s_{i+2}(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. Applying this argument repeatedly leads to the conclusion, that there needs to be an interval on which $\llbracket \alpha \rrbracket$ holds before the next open interval. The fact that σ is non-zeno, furthermore, implies that there is a future open interval. Thus, we can conclude that there is a sequence of singleton intervals starting at interval i such that $\llbracket \alpha \rrbracket$ (and thus α) holds on the last interval in that sequence. Thus, $\sigma^{(i,t)} \models \mathbf{F}_{\leq 0}^s \alpha$.

In both cases we were able to demonstrate that $\sigma^{(i,t)} \models \mathbf{F}_{\leq 0}^s \alpha$. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{< n}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket$ is set to **false** globally.

Now take a $\mathcal{SF}_{< n}^s \alpha$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \mathbf{F}_{< n}^s \alpha$.

Choose $j \in \mathbb{N}$ as large as possible such that $0 \leq j \leq i$ and either R_c holds at interval $j - 1$ or $j = 0$. We now know that (i) $s_j(c) = 0$ and (ii) $s_j(\text{leftto}) = \mathbf{true}$ iff I_j is open. Let $\bar{j} = j + 1$ if interval j is a singleton and $\bar{j} = j$ otherwise. If now $j < i$, then we know that R_c does not hold on interval $i - 1$ meaning that $s_{i-1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$, $s_i(\llbracket \alpha \rrbracket) = \mathbf{false}$ and $s_{i-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$ if I_{i-1} is open. Applying the same reasoning repeatedly, we can deduce

that, firstly, $s_j(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \dots = s_i(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$ and, secondly, $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_i(\llbracket \alpha \rrbracket) = \mathbf{false}$.

Let $\bar{i} = i + 1$ if I_i is a singleton and $\bar{i} = i$ otherwise. Now assume that $s_{\bar{i}}(\llbracket \alpha \rrbracket) = s_{\bar{i}+1}(\llbracket \alpha \rrbracket) = \dots = \mathbf{false}$. In this case Constraints 4 and 5 imply that $s_{\bar{i}}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = s_{\bar{i}+1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \dots = \mathbf{true}$. Thus R_c is **false** on intervals $\bar{i}, \bar{i} + 1, \dots$. As we assumed a non-zeno trace, this implies that there is no upper bound to the value of c on the intervals $\bar{i}, \bar{i} + 1, \dots$ implying that T_c eventually becomes **false** on all intervals starting from some interval after interval \bar{i} . As now $\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket$ holds globally and $\llbracket \alpha \rrbracket$ globally does not hold starting from interval \bar{i} , this contradicts Constraint 9. Thus, assuming there is no point at which $\llbracket \alpha \rrbracket$ holds after interval \bar{i} leads to a contradiction, implying that there has to be a point where $\llbracket \alpha \rrbracket$ holds. Thus, we can pick $k \geq \bar{i}$ as small as possible such that $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$.

- Case 1: $i = k$. As $k \geq \bar{i}$, this implies that I_i is open. As, furthermore, $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$ and thus $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$ we know that $\sigma^{(i,t)} \models \mathbf{F}_{< n}^s \alpha$.
- Case 2: $i \neq k$ and $k = j + 1$. As $j \leq i \leq k$ we know know that $i = j$. Now
 - If I_i is a singleton, then $\sigma^{(i,t)} \models \mathbf{F}_{< n}^s \alpha$ trivially holds.
 - If I_i is open, then $\bar{i} = i$. Thus, by the choice of k we know that $s_i(\llbracket \alpha \rrbracket) = \mathbf{false}$. As $s_i(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$, Constraint 9 implies that T_c holds at interval i . As $j = i$, we know that $s_i(c) = 0$. By the definition of T_c , we now know that the value of δ at interval i is less than or equal to n . This together with the fact that I_i is open implies we can pick a point in I_k that is less than n time units away from (i, t) and, ultimately, that $\sigma^{(i,t)} \models \mathbf{F}_{< n}^s \alpha$.
- Case 3: $i \neq k$ and $k \geq j + 2$. By $s_{\bar{i}}(\llbracket \alpha \rrbracket) = \dots = s_{k-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$ and by Constraints 4 and 5, we now know that $s_{i+1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \dots = s_{k-1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$. Together with our previous observations we now know that $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{k-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$ and $s_j(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \dots = s_{k-1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$. This implies that R_c does not hold on intervals $j, \dots, k - 2$, in turn implying that c and leftto are updated according to Constraint 8 on the transitions from intervals $j, \dots, k - 2$ to the respective following interval. Therefore, $s_{k-1}(c)$ is the difference between the left bound of I_j and the left bound of I_{k-1} . Thus, $s_{k-1}(c) + s_{k-1}(\delta)$ is the difference between the left bound of I_k and the left bound of I_j . As $s_{k-1}(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) = \mathbf{true}$ and $s_{k-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$, Constraint 9 implies that T_c holds at interval $k - 1$. Now
 - If I_j is open, then the difference between the left bounds of I_k and I_j is less than or equal to n . Then we can for every point in I_j pick another point in I_k that is less than n time units away from the point in I_j .

- If I_j is a singleton, then the difference between the left bounds of I_k and I_j is less than n . Again, this means that we can for every point in I_j pick another point in I_k that is less than n time units away from the point in I_j .

Finally, as $j \leq i \leq k$, we can also for (i, t) pick a point in I_k that is less than n time units away. As $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$, this implies that $\sigma^{(i,t)} \models \mathbf{F}_{<n}^s \alpha$.

In each case we were able to demonstrate that $\sigma^{(i,t)} \models \mathbf{F}_{<n}^s \alpha$. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{\leq n}^s$. The proof for $\mathbf{Op} = \mathbf{F}_{\leq n}^s$ proceeds precisely as the proof for $\mathbf{Op} = \mathbf{F}_{<n}^s$, except for arguing that there are time points $\leq n$ time units apart in I_j and I_k in Case 3.

By the definition of T_c for $\triangleleft = <$ and as T_c holds at interval $k - 1$ we know that in Case 3 one of the following:

- The difference between the left bound of I_j is less than n time units. In this case, we can trivially pick for any point in I_j a point that is $\leq n$ time units away in I_k .
- The difference between the left bound of I_j is n time units and I_j open or I_k is a singleton. Again we can pick for any point in I_j a point that is $\leq n$ time units away in I_k .

Proof: For $\mathbf{Op} = \mathbf{U}_{>n}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket$ and *oblig* are set to false globally.

Now take a $\mathcal{S}_{\alpha \mathbf{U}_{>n}^s \beta}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1 v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$.

By the fact that $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \mathbf{true}$ and Constraint 10 we know that $s_i(\text{oblig}) = \mathbf{true}$. Let $\bar{i} = i$ if I_i is open and $\bar{i} = i + 1$ otherwise. Now

- Case 1: \hat{r} holds on interval $i + 1$. Then T_c and $\llbracket \beta \rrbracket$ hold on interval $i + 1$. As $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \mathbf{true}$, we know that $s_{i+1}(c) = 0$ and $s_{i+1}(\text{righto}) = \mathbf{true}$ iff I_i is open. Now
 - If interval I_{i+1} is a singleton, then $s_{i+1}(c) + s_{i+1}(\delta) = 0$. Because T_c holds on interval $i + 1$, we then know that $n = 0$ and $s_{i+1}(\text{righto}) = \mathbf{true}$, the latter implying that I_i is open. Now Constraint 12 implies that $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$. Furthermore, as I_i is open, we can pick a point that is more than 0 time units away from (i, t) in I_{i+1} . Thus, $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$.
 - If, in contrast, I_{i+1} is open then I_i is a singleton and $s_{i+1}(\text{righto}) = \mathbf{false}$. Thus, the fact that T_c is satisfied on interval $i + 1$ implies that $s_{i+1}(\delta) > n$. Thus we can pick a point that is more than n time units away from (i, t) in I_{i+1} . As I_i is a

singleton and I_{i+1} an open interval, Constraint 13 implies that $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$, meaning that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$.

- Case 2: \hat{r} does not hold on interval $i + 1$ and $s_{i+1}(\text{oblig}) = \mathbf{false}$. Now based on Constraint 11 this means that $n = 0$. Furthermore, the only way to satisfy Constraints 12 and 13 is if I_i is open and \hat{r} and $\llbracket \alpha \rrbracket$ hold at interval i . In this case, $s_i(\llbracket \alpha \rrbracket) = s_i(\llbracket \beta \rrbracket) = \mathbf{true}$, implying that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>0}^s \beta$.
- Case 3: \hat{r} does not hold on interval $i + 1$ and $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{false}$. Again, Constraint 11 implies that $n = 0$. Furthermore, Constraints 12 and 13 can only be satisfied if I_i is open and both α and \hat{r} hold on interval i . Clearly, $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>0}^s \beta$.
- Case 4: \hat{r} does not hold on interval $i + 1$, $s_{i+1}(\text{oblig}) = s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$ and \hat{r} holds on interval $i + 2$ or any later interval. Pick j as small as possible such that $j \geq i + 2$ and \hat{r} holds at interval j . Let $\bar{j} = j$ if I_j is open and $\bar{j} = j - 1$ if I_j is a singleton. Note that Constraints 12 and 13 correspond to Constraints 1 and 2 in the \mathbf{U}^s -encoding, except that $\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket$ has been replaced by *oblig* and $\llbracket \beta \rrbracket$ has been replaced by \hat{r} . This correspondence allows us to conclude that $\alpha \mathbf{U}^s \hat{r}$ is satisfied everywhere on interval $i + 1$. By the fact that $\alpha \mathbf{U}^s \hat{r}$ holds on interval $i + 1$ and the choice of j we now know that $s_{i+2}(\llbracket \alpha \rrbracket) = \dots = s_{\bar{j}}(\llbracket \alpha \rrbracket) = \mathbf{true}$. Furthermore, we assumed $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$. Also, if I_i is open, the fact that $s_i(\text{oblig}) = \mathbf{true}$ and Constraint 12 imply that $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$. Thus, we know that $s_{\bar{i}}(\llbracket \alpha \rrbracket) = \dots = s_{\bar{j}}(\llbracket \alpha \rrbracket) = \mathbf{true}$. Now choose k as large as possible such that $i \leq k < j$ and $s_k(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \mathbf{true}$. Now the values of c and *righto* are set according to Constraint 14 on interval $k + 1$ and according to Constraint 15 on intervals $k + 2, \dots, j$. This implies that $s_j(c)$ is the difference between the left bound of I_j and the right bound of I_k . Thus, $s_j(c) + s_j(\delta)$ is the difference between the right bounds of I_j and I_k . Furthermore, $s_j(\text{righto}) = \mathbf{true}$ iff I_k is open. As \hat{r} holds on interval j , we know by the definition of \hat{r} that T_c holds on interval j . Thus, the difference between the right bounds of I_j and I_k is greater or equal to n and greater than n if I_k is a singleton. This implies, that for every point in I_k we can pick a point in I_j that is more than n time units away. As $i \leq k$, we can also pick a point in I_j that is more than n time units away from t . Furthermore, by \hat{r} holding on interval j we know that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$. Together with the fact that $s_{\bar{i}}(\llbracket \alpha \rrbracket) = \dots = s_{\bar{j}}(\llbracket \alpha \rrbracket) = \mathbf{true}$, this implies that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$.
- Case 5: \hat{r} does not hold on intervals $i + 1, i + 2, \dots$ and $s_{i+1}(\text{oblig}) = s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$. Now by Constraints 12 and 13 we know that $s_{\bar{i}}(\llbracket \alpha \rrbracket) = s_{i+1}(\llbracket \alpha \rrbracket) =$

$\dots = \mathbf{true}$ and $s_{\bar{i}}(\mathit{oblig}) = s_{\bar{i}+1}(\mathit{oblig}) = \dots = \mathbf{true}$, i.e. $\llbracket \alpha \rrbracket$ and oblig hold globally starting from interval \bar{i} . Thus, $\neg \mathit{oblig}$ holds only on finitely many intervals. By fairness constraint $\mathcal{F}_{\alpha \mathbf{U}_{>n}^s \beta}$, this implies that $\llbracket \beta \rrbracket$ holds on infinitely many intervals. As σ is non-zeno, this implies that we can pick an interval that contains a point more than n time units away from (i, t) and on which $\llbracket \beta \rrbracket$ holds. As $\llbracket \alpha \rrbracket$ holds globally starting from interval \bar{i} , this implies that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$.

In each case, we were able to demonstrate that $\sigma^{(i,t)} \models \alpha \mathbf{U}_{>n}^s \beta$. ■

Proof: For $\mathbf{Op} = \mathbf{U}_{\geq n}^s$. As a first observation, we note that in case of $\mathbf{Op} = \mathbf{U}_{\geq n}^s$ we know that $n > 0$, as we use the \mathbf{U}^s encoding to encode $\alpha \mathbf{U}_{\geq 0}^s \beta$.

We obtain the $\mathbf{Op} = \mathbf{U}_{\geq n}^s$ proof from the $\mathbf{Op} = \mathbf{U}_{>n}^s$ proof by the following modifications:

- In Case 1, assuming I_{i+1} to be a singleton contradicts our observation that $n > 0$, meaning that I_{i+1} is open, I_i is a singleton. Now the fact that T_c holds on interval $i + 1$ implies that $s_{i+1}(\delta) > n$. This allows us to pick a point in I_i that is $\geq n$ time units away from (i, t) . Analogously to the $\mathbf{Op} = \mathbf{U}_{>n}^s$ proof this leads to $\sigma^{(i,t)} \models \alpha \mathbf{U}_{\geq n}^s \beta$.
- Cases 2 and 3 contradict $n > 0$.
- In Case 4, the fact that T_c holds on interval j implies that either (i) the difference between the right bounds of I_j and I_k is greater than n or (ii) the right bounds of I_j and I_k equals n and I_k is open or I_j is a singleton. Thus, we can for every point in I_k pick a point in I_j that is $\geq n$ time units away.
- Case 5 does not need modification. ■

Proof: For $\mathbf{Op} = \mathbf{R}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \alpha \mathbf{R}^s \beta \rrbracket$ and oblig are set to false globally.

Now take a $\mathcal{S}_{\alpha \mathbf{R}^s \beta}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \alpha \mathbf{R}^s \beta$. Let $\bar{i} = i$ if I_i is open and $\bar{i} = i + 1$ if I_i is a singleton.

As a **first case** assume $s_{\bar{i}}(\llbracket \alpha \rrbracket) = s_{\bar{i}+1}(\llbracket \alpha \rrbracket) = \dots = \mathbf{false}$. Then by Constraints 16, 17 and 18 we know that $s_{\bar{i}}(\mathit{oblig}) = s_{\bar{i}+1}(\mathit{oblig}) = \dots = \mathbf{true}$. Now Constraint 19 implies that $s_{\bar{i}}(\llbracket \beta \rrbracket) = s_{\bar{i}+1}(\llbracket \beta \rrbracket) = \dots = \mathbf{true}$. Clearly, in this case $\sigma^{(i,t)} \models \alpha \mathbf{R}^s \beta$.

As a **second case** assume $\llbracket \alpha \rrbracket$ holds at interval \bar{i} or any later interval. Then let $j \geq \bar{i}$ be as small as possible such that $s_j(\llbracket \alpha \rrbracket) = \mathbf{true}$. Then by Constraints 16, 17 and 18, we know that $s_{\bar{i}}(\mathit{oblig}) = \dots = s_j(\mathit{oblig}) = \mathbf{true}$. Now

- If I_j is open, then by Constraint 19 we have that $s_{\bar{i}}(\llbracket \beta \rrbracket) = \dots = s_{j-1}(\llbracket \beta \rrbracket) = \mathbf{true}$. This, in turn, implies that for any time point after (i, t) at which $\llbracket \beta \rrbracket$ does not hold there is an earlier time point in interval j . Hence, $\sigma^{(i,t)} \models \alpha \mathbf{R}^s \beta$.

- If I_j is a singleton, then by Constraint 19 we have that $s_{\bar{i}}(\llbracket \beta \rrbracket) = \dots = s_j(\llbracket \beta \rrbracket) = \mathbf{true}$. Thus, the single time point in interval j , at which $\llbracket \alpha \rrbracket$ holds, lies in between time point (i, t) and any potential future point at which $\llbracket \beta \rrbracket$ does not hold. Again, $\sigma^{(i,t)} \models \alpha \mathbf{R}^s \beta$. ■

Proof: For $\mathbf{Op} = \mathbf{G}_{\leq 0}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket$ is set to false globally.

Now take a $\mathcal{S}_{\mathbf{G}_{\leq 0}^s \alpha}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \mathbf{G}_{\leq 0}^s \alpha$.

Recall, that by the semantics of $\mathbf{G}_{\leq n}^s$, a point on a trace satisfies $\mathbf{G}_{\leq 0}^s \alpha$ iff all *future* points that are zero time units away from that point satisfy α . Note that a future time point can be zero time units away only if both the current and the next interval are singletons.

By Constraint 20, there are two possibilities:

- I_i or I_{i+1} is open. In this case, there are no future time points that are zero time units away for any point on interval i . Hence, $\sigma^{(i,t)} \models \mathbf{G}_{\leq 0}^s \alpha$ trivially.
- I_i and I_{i+1} are both singletons and $s_{i+1}(\llbracket \alpha \rrbracket) = s_{i+1}(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. By the fact that $s_{i+1}(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$, we can again deduce that either I_{i+2} is open or $s_{i+2}(\llbracket \alpha \rrbracket) = s_{i+2}(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$. Repeatedly applying this argument leads to the conclusion that $\llbracket \alpha \rrbracket$ has to hold on all future singletons up to the next open interval, i.e., all future intervals containing points zero time units away from (i, t) . Thus, $\sigma^{(i,t)} \models \mathbf{G}_{\leq 0}^s \alpha$.

In both cases, we were able to show that $\sigma^{(i,t)} \models \mathbf{G}_{\leq 0}^s \alpha$. ■

Proof: For $\mathbf{Op} = \mathbf{G}_{<n}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \mathbf{G}_{<n}^s \alpha \rrbracket$ and oblig are set to false globally.

Now take a $\mathcal{S}_{\mathbf{G}_{<n}^s \alpha}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1, v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \mathbf{G}_{<n}^s \alpha \rrbracket) = \mathbf{true}$. It remains to show that $\sigma^{(i,t)} \models \mathbf{G}_{<n}^s \alpha$.

Take an arbitrary $j > i$ and $t_2 \in I_j$ such that $t_2 - t < n$ (if such an j exists). Let k be as large as possible such that $i \leq k < j$ and $s_k(\llbracket \mathbf{G}_{<n}^s \alpha \rrbracket) = \mathbf{true}$. By Constraint 22, we know that $s_{k+1}(c) = 0$. Furthermore, by Constraints 22 and 23, we know that $s_j(c)$ is the difference between the right bound of I_k and the left bound I_j . As $k \geq i$ and $t_2 - t < n$, we know that this difference must be less than n and, consequently, T_c holds on interval j . By Constraint 21, this implies that $s_j(\llbracket \alpha \rrbracket) = \mathbf{true}$. As we picked j to be an arbitrary interval containing a point less than n time units away from (i, t) , we can conclude that $\llbracket \alpha \rrbracket$ holds at any point on intervals $i + 1, i + 2, \dots$ that is less than n time units after (i, t) .

Additionally, Constraint 21 ensures that $\llbracket \alpha \rrbracket$ also holds on interval i , if that interval is open. Thus, it is guaranteed that $\llbracket \alpha \rrbracket$ holds at all future points less than n time units away and $\sigma^{(i,t)} \models \mathbf{G}_{<n}^s \alpha$. ■

Proof: For $\mathbf{Op} = \mathbf{G}_{<n}^s$. We modify the proof for $\mathbf{G}_{<n}^s$ by picking $j > i$, $t_2 \in I_j$ with $t_2 - t \leq n$. Then we know that the difference between the left bound of I_j and the right bound of I_i is less than or equal to n and can be equal to n only if both intervals are singletons. Now

- if $s_j(c) < n$ then T_c is satisfied on interval j and we proceed as before.
- if $s_j(c) = n$ then we know that $s_j(c)$ is precisely the difference between the left bound of I_j and the right bound of I_i and I_i and I_j are both singletons. Now, $k = i$ or there is a sequence of intervals $I_i I_{i+1} \dots I_k$ that are all singletons. In either case, I_k is a singleton and $s_j(\text{righto}) = \text{false}$. Thus, T_c is satisfied also in this case and we continue as before. ■

Proof: For $\mathbf{Op} = \mathbf{R}_{>n}^s$. The “preservation of traces” property follows from the fact that the constraints can easily be satisfied globally when $\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket$ and oblig are set to false globally.

Now take a $\mathcal{S}_{\alpha \mathbf{R}_{>n}^s \beta}$ run $\tau = s_0 s_1 s_2 \dots$ with $\text{trace}(\tau) = \sigma = \langle I_0 v_0 \rangle \langle I_1 v_1 \rangle \dots$, $i \in \mathbb{N}$ and $t \in I_i$ with $s_i(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \text{true}$. It remains to show that $\sigma^{(i,t)} \models \alpha \mathbf{R}_{>n}^s \beta$. As usual, let $\bar{i} = i$ if interval i is open and $\bar{i} = i + 1$ otherwise.

As a **first case** assume that for all $(j, t_2) \in T(\sigma)$ with $t_2 - t > n$ we have that $s_j(\llbracket \beta \rrbracket) = \text{true}$. In this case, we trivially have $\sigma^{(i,t)} \models \alpha \mathbf{R}_{>n}^s \beta$.

As a **second case**, assume there is $(j, t_2) \in T(\sigma)$ with $t_2 - t > n$ and $s_j(\llbracket \beta \rrbracket) = \text{false}$.

- Case 2.a: $i = j$: As $t_2 - t > n$, this implies that $\delta > n$ at interval i . Then, Constraint 28 implies that $s_i(\llbracket \alpha \rrbracket) = \text{true}$. As interval i also has to be open to allow δ to be non-zero, we now know that there is point in between (i, t) and (j, t_2) where $\llbracket \alpha \rrbracket$ holds.
- Case 2.b: $i < j$ and $s_j(\text{oblig}) = \text{false}$. Analogously to the proof of the lemma for the untimed \mathbf{R}^s encoding, $s_j(\text{oblig}) = \text{false}$ implies that $\llbracket \alpha \rrbracket$ holds at some point in between (i, t) and (j, t_2) .
- Case 2.c: $i < j$ and $s_j(\text{oblig}) = s_j(\llbracket \alpha \rrbracket) = \text{true}$ and I_j is open. Then, as I_j is open and $s_j(\llbracket \alpha \rrbracket) = \text{true}$, we know that $\llbracket \alpha \rrbracket$ holds at some point in between (i, t) and (j, t_2) .
- Case 2.d: $i < j$ and $s_j(\text{oblig}) = \text{true}$ and either I_j is a singleton or $s_j(\llbracket \alpha \rrbracket) = \text{false}$. Then, according to Constraints 27 we know T_c does not hold on interval j . Now pick $k \leq j$ as large as possible such that $s_k(c) = 0$ and one of the following:
 - D_c holds at interval $k - 1$
 - R_c holds at interval $k - 1$, or

– $k = 0$

Now Constraint 31 implies that $s_j(c)$ is the difference between the left bound of I_j and the left bound of I_k . Consequently, $s_j(c) + s_j(\delta)$ is the difference between the right bound of I_j and the left bound of I_k . Now by the fact that T_c does not hold we know that the difference between the right bound of I_j and the left bound of I_k is less than or equal to n time units. Furthermore, $t_2 - t > n$ implies that the difference between the right bound of I_j and the left bound of I_i is greater than n . This, in turn, implies that $k > i$ and at least one of the intervals $I_i, I_{i+1}, \dots, I_{k-1}$ is open. This implies that $k > \bar{i} > 0$. Now, there are three possibilities:

- R_c holds at interval $k - 1$ and $s_{k-1}(\llbracket \alpha \rrbracket) = \text{true}$. Then there is a point in between (i, t) and (j, t_2) at which α holds.
- R_c holds at interval $k - 1$ and $s_{k-1}(\llbracket \alpha \rrbracket) = \text{false}$. By the definition of R_c now $s_{k-1}(\text{oblig}) = \text{false}$. analogously to the untimed \mathbf{R}^s encoding and Case 2.b, this implies that $\llbracket \alpha \rrbracket$ holds on an interval in the range $\bar{i}, \dots, k - 1$.
- D_c holds at interval $k - 1$. This implies that $s_{k-1}(\llbracket \alpha \rrbracket) = \text{true}$.

In each of the mentioned cases, we were able to show $\llbracket \alpha \rrbracket$ holds at some point in between (i, t) and (j, t_2) , allowing us to conclude that $\sigma^{(i,t)} \models \alpha \mathbf{R}_{>n}^s \beta$. ■

Proof: For $\mathbf{Op} = \mathbf{R}_{\geq n}^s$. To adapt the $\mathbf{R}_{>n}^s$ proof for $\mathbf{R}_{\geq n}^s$ modify the second case as follows. We pick a $(j, t_2) \in T(\sigma)$ with $s_j(\llbracket \beta \rrbracket) = \text{false}$ and $t_2 - t \geq n$. Cases 2.a to 2.c do not require substantial changes. In Case 2.d, we pick k as before.

We now observe that $t_2 - t \geq n$ implies that the difference between the right bound of I_j and the left bound of I_i is greater than or equal to n . Furthermore, the difference can only be equal if I_i and I_j are both singletons.

The fact that T_c does not hold at interval j implies that $s_j(c) + s_j(\delta) \leq n$. Furthermore, if $s_j(c) + s_j(\delta) = n$ then we know that I_j is open or $s_j(\text{leftto}) = \text{true}$.

Now

- If the difference between the right bound of I_j and the left bound of I_i is greater than n , we again can conclude that $k > \bar{i}$ and proceed as before.
- Likewise, if $s_j(c) + s_j(\delta) < n$ we conclude that $k > \bar{i}$ and proceed as before.
- If the difference between the right bound of I_j and the left bound of I_i equals n and $s_j(c) + s_j(\delta) = n$, then our previous observations tell us that (i) I_i and I_j are singletons (ii) $s_j(\text{leftto}) = \text{true}$. Furthermore, as $n > 0$, $s_j(c) + s_j(\delta) = n$, $s_k(c) = 0$ and I_j is a singleton we know that $k < j$. As the value of leftto on intervals $k + 1, \dots, j$ set according to Constraint 31, we know that $s_k(\text{leftto}) = \text{true}$. This eliminates the

possibilities that $k = 0$ or that D_c holds on interval $k - 1$, leaving only the possibility that R_c holds on interval $k - 1$. Then by Constraint 30, I_k is open. Together with our assumptions about the left-bound-to-right-bound differences and the fact that I_i is a singleton, this implies that $k > i$. Finally, as I_i is a singleton and $s_i(\llbracket \alpha \mathbf{R}_{\geq n}^s \beta \rrbracket) = \mathbf{true}$, R_c does not hold on interval i , meaning that $k > i + 1 = \bar{i}$. Now we can continue as previously. ■

F. Completeness proofs

Lemma 5: The transition system \mathcal{S}_p is a complete encoding for p , $\mathcal{S}_{\neg p}$ is a complete encoding for $\neg p$. If a transition system \mathcal{S} over AP is a complete encoding of α and β , then the transition system $\mathcal{S}_{\mathbf{Op}\alpha}$ over AP is a complete encoding of $\mathbf{Op} \alpha$ for each $\mathbf{Op} \in \{\mathbf{F}_{\leq 0}^s, \mathbf{F}_{< n}^s, \mathbf{F}_{\leq n}^s, \mathbf{G}_{\leq 0}^s, \mathbf{G}_{< n}^s, \mathbf{G}_{\leq n}^s\}$, and $\mathcal{S}_{\alpha \mathbf{Op} \beta}$ is a complete encoding of $\alpha \mathbf{Op} \beta$ for each $\mathbf{Op} \in \{\wedge, \vee, \mathbf{U}^s, \mathbf{U}_{\geq n}^s, \mathbf{U}_{> n}^s, \mathbf{R}^s, \mathbf{R}_{\geq n}^s, \mathbf{R}_{> n}^s\}$.

Recall, that an encoding \mathcal{S}_ϕ is complete if for every ϕ -fine trace $\sigma = \langle I_0, v_0 \rangle \langle I_1, v_1 \rangle \langle I_2, v_2 \rangle \dots$ in $\text{traces}(\mathcal{S})$, there is a run $\tau = s_0 s_1 s_2 \dots$ in \mathcal{S}_ϕ such that $\text{trace}(\tau) = \sigma$ and for all points (i, t) in σ it holds that $\sigma^{(i, t)} \models \phi$ implies $v_i(\llbracket \phi \rrbracket) = \mathbf{true}$. Thus, we can prove completeness by assuming a ϕ -fine trace $\sigma \in \text{traces}(\mathcal{S})$, extending it to a run τ by giving values for the auxiliary variables used in the encoding (setting $\llbracket \phi \rrbracket$ to \mathbf{true} exactly on those intervals where ϕ holds) and then arguing that all constraints of the encoding are satisfied. Lemma 5 is proven by structural induction. That is, it will be assumed that the lemma holds for the subformulas α and β . Like Lemma 4, we will prove Lemma 5 separately for each operator.

As the lemma assumes ϕ -finess, ϕ either holds at all points in a given interval in σ or ϕ does not hold at any point inside the interval. We use the notation $\sigma^{(j, \cdot)} \models \phi$ to denote that ϕ is satisfied by all points belonging to interval j and $\sigma^{(j, \cdot)} \not\models \phi$ to denote that no point inside the interval satisfies ϕ .

Proof: For $\mathbf{Op} = \mathbf{U}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) / s_i(\llbracket \alpha \rrbracket) / s_i(\llbracket \beta \rrbracket)$ to \mathbf{true} iff $\sigma^{(i, \cdot)} \models \alpha \mathbf{U}^s \beta / \sigma^{(i, \cdot)} \models \alpha / \sigma^{(i, \cdot)} \models \beta$, respectively.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. Now

- If $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{false}$ then both Constraints 1 and 2 trivially hold at interval i .
- If $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ and I_i is open, then Constraint 2 is trivially satisfied. Furthermore, as $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ we know that $\sigma^{(i, \cdot)} \models \alpha \mathbf{U}^s \beta$. Pick any $t_1 \in I_i$. By the semantics of \mathbf{U}^s we now know that there is a future time point $(j, t_2) \in T_+(\sigma, (i, t))$ such that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ and $\llbracket \alpha \rrbracket$ holds anywhere in between (i, t_1) and (j, t_2) . Note that due to the fact that I_i is open, there is a guarantee that interval i contains time points lying in between (i, t_1) and (j, t_2) , implying

that $s_i(\llbracket \alpha \rrbracket) = \mathbf{true}$. Now if $j = i$ or $j = i + 1$, then Constraint 1 is satisfied. Furthermore, if $j > i + 1$, then also $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$ and $\sigma^{(i+1, \cdot)} \models \alpha \mathbf{U}^s \beta$. Thus, $s_{i+1}(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$, implying that Constraint 2 is satisfied in this case as well.

- If $s_i(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ and I_i is a singleton, then Constraint 1 is trivially satisfied. Let $\{t_1\} = I_i$. Again, we pick a time point $(j, t_2) \in T_+(\sigma, (i, t_2))$ such that $s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ and $\llbracket \alpha \rrbracket$ holds anywhere in between (i, t_1) and (j, t) . Now if $j = i + 1$ and I_j is a singleton, then Constraint 2 is satisfied. If $j = i + 1$ and I_j is open, then $s_j(\llbracket \alpha \rrbracket) = s_j(\llbracket \beta \rrbracket) = \mathbf{true}$ meaning that $\sigma^{(j, \cdot)} \models \alpha \mathbf{U}^s \beta$. Then $s_j(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ and Constraint 2 is satisfied. If $j > i + 1$ then we observe that $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$ and $\sigma^{(i+1, \cdot)} \models \alpha \mathbf{U}^s \beta$, meaning that $s_{i+1}(\llbracket \alpha \mathbf{U}^s \beta \rrbracket) = \mathbf{true}$ and Constraint 2 is satisfied in this case as well.

The fairness condition is satisfied: It is easy to see that now the fairness constraint $\mathcal{F}_{\alpha \mathbf{U}^s \beta}$ holds as well. We set $\llbracket \alpha \mathbf{U}^s \beta \rrbracket$ to \mathbf{true} precisely on those intervals on which $\alpha \mathbf{U}^s \beta$ holds, implying that there is a future point at which β holds. Thus, if $\llbracket \alpha \mathbf{U}^s \beta \rrbracket$ holds on all intervals starting from some point, then $\alpha \mathbf{U}^s \beta$ holds globally starting from that point. Hence, there is always a future interval at which β holds, meaning that β (and thus $\llbracket \beta \rrbracket$) holds infinitely often. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{\leq 0}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) / s_i(\llbracket \alpha \rrbracket)$ to \mathbf{true} iff $\sigma^{(i, \cdot)} \models \mathbf{F}_{\leq 0}^s \alpha / \sigma^{(i, \cdot)} \models \alpha$, respectively.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. If $s_i(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{false}$, then Constraint 3 is trivially satisfied. If, in contrast, $s_i(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$, then we know that $\sigma^{(i, \cdot)} \models \mathbf{F}_{\leq 0}^s \alpha$. Thus, there is a $j > i$ such that $s_j(\llbracket \alpha \rrbracket) = \mathbf{true}$ and for every point in I_{i+1} there is a point in I_j that is at most 0 time units away. The latter implies that intervals I_i, \dots, I_j are all singletons. Thus, in particular, I_i and I_{i+1} are singletons. Furthermore, if $j = i + 1$, then $s_{i+1}(\llbracket \alpha \rrbracket) = \mathbf{true}$, implying that Constraint 3 is satisfied at interval i . If, in contrast $j > i + 1$ then $\sigma^{(i+1, \cdot)} \models \mathbf{F}_{\leq 0}^s \alpha$ as well, implying that $s_{i+1}(\llbracket \mathbf{F}_{\leq 0}^s \alpha \rrbracket) = \mathbf{true}$ and, ultimately, that Constraint 3 is satisfied at interval i also in this case. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{< n}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \mathbf{F}_{< n}^s \alpha \rrbracket) / s_i(\llbracket \alpha \rrbracket)$ to \mathbf{true} iff $\sigma^{(i, \cdot)} \models \mathbf{F}_{< n}^s \alpha / \sigma^{(i, \cdot)} \models \alpha$, respectively. Furthermore, we set $s_0(c) = 0$ and $s_0(\text{leftto}) = \mathbf{false}$. For $i > 0$ we set $s_i(c)$ and $s_i(\text{leftto})$ according to Constraints 7 and 8 and s_{i-1} .

The initial constraint is satisfied: Initial constraint $\mathcal{I}_{\mathbf{F}_{< n}^s \alpha}$ is trivially satisfied as $s_0(c) = 0$ and $s_0(\text{leftto}) = \mathbf{false}$.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. Let $\bar{i} = i$ if I_i is open and $\bar{i} = i + 1$ if I_i is a singleton. Now we will show that interval i satisfies Constraints 4 and 5 using a case distinction.

- If $s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{false}$ or $s_{i+1}(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$ then Constraints 4 and 5 are trivially satisfied.
- If $s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$ and $s_{i+1}(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{false}$, then we know that $\sigma^{(i,\cdot)} \models \mathbf{F}_{<n}^s \alpha$ and $\sigma^{(i+1,\cdot)} \not\models \mathbf{F}_{<n}^s \alpha$. Now
 - If I_i is open then Constraint 5 is trivially satisfied. Furthermore, by semantics of $\mathbf{F}_{<n}^s$ we know that $\sigma^{(i,\cdot)} \models \mathbf{F}_{<n}^s \alpha$ and $\sigma^{(i+1,\cdot)} \not\models \mathbf{F}_{<n}^s \alpha$ implies that $s_i(\llbracket \alpha \rrbracket) = \text{true}$ or $s_i(\llbracket \alpha \rrbracket) = \text{true}$. In either case, Constraint 4 is satisfied.
 - If I_i is a singleton then Constraint 4 is trivially satisfied. Furthermore, by semantics of $\mathbf{F}_{<n}^s$ we know that $\sigma^{(i,\cdot)} \models \mathbf{F}_{<n}^s \alpha$ and $\sigma^{(i+1,\cdot)} \not\models \mathbf{F}_{<n}^s \alpha$ implies that (i) I_{i+1} is a singleton as well and (ii) $s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$. Thus, Constraint 5 is satisfied as well.

It remains to be shown that Constraint 9 holds on interval i , which will be done by contradiction. Assume, Constraint 9 does not hold on interval i . Then, T_c does not hold on interval i , $s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$ and I_i is a singleton or $s_i(\llbracket \alpha \rrbracket) = \text{false}$. As $s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$, we know that $\sigma^{(i,\cdot)} \models \mathbf{F}_{<n}^s \alpha$. Pick $j \leq i$ as large as possible such that R_c holds at interval $j - 1$ is such j exists and set $j = 0$ otherwise. Now we know that $s_j(c) = 0$ and $s_j(\text{leftto}) = \text{true}$ iff I_j is open.

- If $j = i$, then we know that the value of $s_i(c) = 0$. Now
 - If I_i is a singleton, then the value of δ at interval i is 0 as well, which implies that T_c contrary to our assumption satisfied on interval i .
 - If I_i is open, then our assumption that Constraint 9 does not hold implies that $s_i(\llbracket \alpha \rrbracket) = \text{false}$. As $\sigma^{(i,\cdot)} \models \mathbf{F}_{<n}^s \alpha$, we now know that δ at interval i can be at most n , implying that T_c is satisfied and contradicting our assumption that Constraint 9 does not hold.
- If $j < i$, then we know by the fact that R_c does not hold on intervals $j, \dots, i - 1$ that the value of c at intervals $j + 1, \dots, i$ has been set according to Constraint 8. Hence, $s_i(c)$ is the difference between the left bound of I_i and the left bound of I_j . Furthermore, $s_i(c) + s_i(\delta)$ is the difference between the right bound of I_i and the left bound of I_j and $s_i(\text{leftto}) = \text{true}$ iff I_j is open. By the fact that R_c does not hold on intervals $j, \dots, i - 1$ and the fact that $s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$ we know that $s_j(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \dots = s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$. Let $\bar{j} = j$ if I_j is open and $\bar{j} = j + 1$ if I_j is a singleton. As R_c does not hold on intervals $j, \dots, i - 1$ and $s_j(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \dots = s_i(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$ we know that $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_i(\llbracket \alpha \rrbracket) = \text{false}$. As $s_j(\llbracket \mathbf{F}_{<n}^s \alpha \rrbracket) = \text{true}$, we know that $\sigma^{(j,\cdot)} \models \mathbf{F}_{<n}^s \alpha$. Thus, for each point in I_j there is a future point at which α holds and that is less than n time units away. As $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_i(\llbracket \alpha \rrbracket) = \text{false}$, this implies that

every point in I_j is less than n time units away from a time point in I_{i+1} . Thus, the difference between the right bound of I_i and the left bound of I_j is less than n time units if I_j is a singleton and less than or equal to n time units if I_j is open. Recalling that the value of $c + \delta$ at interval i is precisely said difference and $s_i(\text{leftto}) = \text{true}$ if I_j is open, we conclude that T_c is satisfied at interval i , contradicting our assumption.

In each case, we were able to show that the assumption that Constraint 9 does not hold leads to a contradiction. ■

Proof: For $\mathbf{Op} = \mathbf{F}_{\leq n}^s$. The only difference between the proof for $\mathbf{F}_{\leq n}^s$ and the proof for $\mathbf{F}_{<n}^s$ is in arguing that Constraint 9 is satisfied.

- The case where $i = j$ and I_i is a singleton does not need modification.
- In the case where $i = j$ and I_i is open, we observe that $\sigma^{(i,\cdot)} \models \mathbf{F}_{\leq n}^s \alpha$ and $s_i(\llbracket \alpha \rrbracket) = \text{false}$. Thus, we know that the value of δ at interval i is at most n . Furthermore, as I_i is open, we know that $s_i(\text{leftto}) = \text{true}$, contradicting the assumption that T_c is not satisfied.
- In the case where $j < i$, we observe that $s_j(\llbracket \alpha \rrbracket) = \dots = s_i(\llbracket \alpha \rrbracket) = \text{false}$ and $\sigma^{(j,\cdot)} \models \mathbf{F}_{\leq n}^s \alpha$. Thus, the difference between the left bound of I_j and the right bound of I_i is less than or equal to n and less than n if I_j is a singleton and I_{i+1} is open, again leading to a contradiction based on the fact that T_c is satisfied. ■

Proof: For $\mathbf{Op} = \mathbf{U}_{>n}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) / s_i(\llbracket \alpha \rrbracket) / s_i(\llbracket \beta \rrbracket)$ to **true** iff $\sigma^{(i,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta / \sigma^{(i,\cdot)} \models \alpha / \sigma^{(i,\cdot)} \models \beta$, respectively. We set $s_0(c) = 0$ and $s_0(\text{rightto}) = \text{false}$. For $i > 0$ we set $s_i(c)$ and $s_i(\text{rightto})$ according to Constraints 14 and 15 and s_{i-1} . Furthermore, we set $s_i(\text{oblig}) = \text{true}$ iff at least one of the following cases holds:

- 1) $\sigma^{(i,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$
- 2) $n > 0$, $i > 0$ and $\sigma^{(i-1,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$,
- 3) $i > 0$, I_{i-1} is open, $s_{i-1}(\text{oblig}) = \text{true}$ and \hat{r} neither holds on interval $i - 1$ nor on interval i .
- 4) $i > 0$, I_{i-1} is a singleton, $s_{i-1}(\text{oblig}) = \text{true}$ and \hat{r} does not hold on interval i or I_i is open.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. Note, that the rules for setting the value of *oblig* ensure that Constraint 10 is satisfied on interval i .

Assume $\sigma^{(i,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$ and $n > 0$. Take $t \in I_i$ such that the difference between the right bound of I_i and t is less than n . Now there is a future time point more than n time units from (i, t) at which β holds and up to which α holds. The fact that this point is more than n time units away implies that either I_{i+1} is open or the time point is on interval $i + 2$ or a later interval. In either case $s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$. Together with the rules for setting the value of *oblig*, this implies that Constraint 11 is satisfied.

If, in contrast, $\sigma^{(i,\cdot)} \not\models \alpha \mathbf{U}_{>n}^s \beta$ then Constraint 11 is trivially satisfied and if $n = 0$, Constraint 11 is not used at all.

Next, we show that Constraints 12 and 13 are satisfied on interval i .

- Assume $s_i(\text{oblig}) = \text{false}$. In this case, Constraints 12 and 13 are trivially satisfied.
- Assume $s_i(\text{oblig}) = s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \text{true}$. Now if I_i is open, then $s_i(\llbracket \alpha \rrbracket) = \text{true}$. Furthermore, by Constraint 14 we know $s_{i+1}(c) = 0$ and $s_{i+1}(\text{righto}) = \text{true}$ iff I_i is open. Now
 - If $s_{i+1}(\text{oblig}) = s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$, then Constraints 12 and 13 are trivially satisfied.
 - If $s_{i+1}(\llbracket \alpha \rrbracket) = \text{false}$, then the fact that $\sigma^{(i,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$ implies that $n = 0$ and one of the following:
 - * $s_i(\llbracket \beta \rrbracket) = \text{true}$ and I_i is open. In this case, $s_i(\delta) > 0$, meaning that T_c and \hat{r} are satisfied on interval i and ultimately that Constraints 12 and 13 are satisfied.
 - * $s_{i+1}(\llbracket \beta \rrbracket) = \text{true}$, I_i is open and I_{i+1} is a singleton. In this case, $s_{i+1}(\text{righto}) = \text{true}$, implying that T_c and \hat{r} are satisfied on interval $i + 1$ and ultimately that Constraints 12 and 13 are satisfied.
 - If $s_{i+1}(\text{oblig}) = \text{false}$ then by the fact that $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \text{true}$ and Rule 2 for setting the value of oblig we know that $n = 0$. If we now assume that I_i is a singleton, then by Rule 4 for setting the value of oblig we know that \hat{r} holds on interval $i + 1$ and I_{i+1} is a singleton. The latter, however, implies that $s_{i+1}(c) + s_{i+1}(\delta) = 0$ and, thus, that \hat{r} does not hold on interval $i + 1$. Thus, assuming I_i to be a singleton leads to a contradiction and we know that I_i is open. Now I_{i+1} is a singleton and we know that $s_{i+1}(c) + s_{i+1}(\delta) = 0$ and \hat{r} is not satisfied on interval $i + 1$. Now Rule 3 for setting the value of oblig and the fact that $s_{i+1}(\text{oblig}) = \text{false}$ imply that \hat{r} holds on interval i . As I_i is open and $\sigma^{(i,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$, now $s_i(\llbracket \alpha \rrbracket) = \text{true}$ and Constraints 12 and 13 are satisfied.
- Assume $s_i(\text{oblig}) = \text{true}$ and $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \text{false}$. Choose $j < i$ as large as possible such that $s_j(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \text{true}$. We know that a corresponding interval exists based on the fact that $s_i(\text{oblig}) = \text{true}$. Let $\bar{j} = j$ if I_j is open and $\bar{j} = j + 1$ otherwise. Now by the choice of j we know $s_j(\text{oblig}) = \dots = s_i(\text{oblig}) = \text{true}$.
 - Assume $n > 0$. Based on the rules for setting the value of oblig , we now know that \hat{r} does not hold on intervals $j + 2, \dots, i$ and not on $j + 1$ either if I_{j+1} is open. Furthermore, if I_{j+1} is a singleton as

$s_{j+1}(c) = 0$ we know that $s_{j+1}(c) + s_{j+1}(\delta) = 0$ meaning T_c (and, thus, \hat{r}) does not hold on interval $j + 1$. Thus, \hat{r} does not hold on intervals $j + 1, \dots, i$.

- Assume $n = 0$. Based on the rules for setting the value for oblig , we now immediately know that \hat{r} does not hold on intervals $j + 1, \dots, i$ and not on interval j either if I_j is open.

Now as $\sigma^{(j,\cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$, we can pick $k \geq j$ such that $s_k(\llbracket \beta \rrbracket) = \text{true}$, for every point in I_j there is a point in I_k that is more than n time units away and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{\bar{k}}(\llbracket \alpha \rrbracket) = \text{true}$ with $\bar{k} = k$ if I_j is open and $\bar{k} = k - 1$ if I_k is a singleton. We observe that $k = j$ is possible only if $n = 0$ and I_j is open. In this case, however, T_c and $\llbracket \beta \rrbracket$ would both hold on interval j , meaning that \hat{r} holds and contradicting our previous observation that \hat{r} does not hold on interval j if I_j is open and $n = 0$. Thus, $k > j$.

Take an arbitrary $m \in \mathbb{N}$ with $j < m \leq i$. Now we note that $s_m(\text{righto}) = \text{true}$ iff I_j is open. Furthermore, $s_m(c)$ is the difference between the left bound of I_m interval and the right bound of I_j . Correspondingly, $s_m(c) + s_m(\delta)$ is the difference between the right bounds of I_m and I_j . Now as \hat{r} does not hold on interval m , we know that either $s_m(\llbracket \beta \rrbracket) = \text{false}$ or T_c does not hold. By the definition of T_c , the latter implies that the difference between the right bounds of I_m and I_j is less than or equal to n and less than n if I_j is open, meaning that there is a point in I_j for which there is no point in I_m that is $> n$ time units away. This allows us to conclude that $k \neq m$. As we picked an $j < m \leq i$ this means that $k > i$ and, thus, $s_i(\llbracket \alpha \rrbracket) = \text{true}$.

- Now if \hat{r} holds on interval $i + 1$ and I_i is open, then Constraints 12 and 13 are satisfied on interval i .
- If \hat{r} holds on interval $i + 1$, I_i is a singleton and I_{i+1} is a singleton, then Constraints 12 and 13 are satisfied on interval i .
- If \hat{r} holds on interval $i + 1$, I_i is a singleton and I_{i+1} is open, according to Rule 4 for setting the value of oblig we have $s_{i+1}(\text{oblig}) = \text{true}$. Furthermore, as $k > i$ and I_{i+1} is open we have $\bar{k} \geq i + 1$, implying that $s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$. Thus, Constraints 12 and 13 are satisfied on interval i .
- If \hat{r} does not hold on interval $i + 1$, then we can use the same argument used to show that $k > i$ to show that, in fact, $k > i + 1$, implying that $s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$. Furthermore, by the Rules 3 and 4 for setting the value of oblig and the fact that \hat{r} does not hold on intervals i and $i + 1$, we also know that $s_{i+1}(\text{oblig}) = \text{true}$. Hence, Constraints 12 and 13 are satisfied on interval i .

The fairness condition is satisfied: It remains to be shown that the fairness constraint $\mathcal{F}_{\alpha \mathbf{U}_{>n}^s \beta}$ is satisfied by our choice of values, which will be done by contradiction. Assume the fairness constraint is not satisfied. Then there is an $i \in \mathbb{N}$ such that $s_i(\text{oblig}) = s_{i+1}(\text{oblig}) = \dots = \text{true}$ and $s_i(\llbracket \beta \rrbracket) = s_{i+1}(\llbracket \beta \rrbracket) = \dots = \text{false}$. As $s_i(\llbracket \beta \rrbracket) = s_{i+1}(\llbracket \beta \rrbracket) = \dots = \text{false}$, we know that intervals $i, i+1, \dots$ do not satisfy $\alpha \mathbf{U}_{>n}^s \beta$ and, thus, $s_i(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = s_{i+1}(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \dots = \text{false}$. By the rules for setting the value of *oblig*, we set *oblig* to **true** only if $\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket$ hold on the current or the previous interval or *oblig* holds on the previous interval. Thus, the fact that $s_i(\text{oblig}) = \text{true}$ implies that there is an interval before interval i on which $\alpha \mathbf{U}_{>n}^s \beta$ holds.

Pick j as large as possible such that $j < i$ and $s_j(\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket) = \text{true}$. Let $\bar{j} = j$ if I_j is open and $\bar{j} = j+1$ if I_j is a singleton. As $\sigma^{(j, \cdot)} \models \alpha \mathbf{U}_{>n}^s \beta$, there is a $k \geq j$ such that $s_k(\llbracket \beta \rrbracket) = \text{true}$, for every point in I_j there is a point in I_k that is more than n time units away and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_k(\llbracket \alpha \rrbracket) = \text{true}$ with $\bar{k} = k$ if I_j is open and $\bar{k} = k-1$ if I_k is a singleton. As $s_i(\llbracket \beta \rrbracket) = s_{i+1}(\llbracket \beta \rrbracket) = \dots = \text{false}$, we know that $k < i$. Recall, that we picked j to be the last interval at which $\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket$ holds. Hence, we know that *oblig* on any later interval can only be set to **true** based on Rules 3 and 4. As both of these rules require *oblig* to hold on the respective previous interval we know that $s_j(\text{oblig}) = s_{j+1}(\text{oblig}) = \dots = \text{true}$.

- Assume that $k = j$. By the semantics of $\mathbf{U}_{>n}^s$, this implies that $n = 0$ and I_i is open. Then T_c is satisfied on interval j . As, additionally, $s_k(\llbracket \beta \rrbracket) = \text{true}$ and, thus, \hat{r} holds, the rules for setting the value of *oblig* imply that $s_{i+1}(\text{oblig}) = \text{false}$, contradicting our observation that $s_j(\text{oblig}) = s_{j+1}(\text{oblig}) = \dots = \text{true}$.
- Assume that $k = j+1$ and $n > 0$. Then I_{j+1} is open and $s_{j+1}(\delta) > n$. Thus, both T_c and $\llbracket \beta \rrbracket$ hold on interval $j+1 = k$, implying that \hat{r} holds. As I_{j+1} is open, our rules for setting the value for *oblig* now imply that $s_{j+2}(\text{oblig}) = \text{false}$, contradicting our observation that $s_j(\text{oblig}) = s_{j+1}(\text{oblig}) = \dots = \text{true}$.
- Assume that $k > j+1$ or $k = j+1$ and $n = 0$. Then *oblig* was set to **true** on interval k by Rule 3 or 4 implying that \hat{r} does not hold on interval k or I_k is open. As *oblig* is set to **true** on interval $k+1$ by Rule 3 or 4 as well, I_k being open again implies that \hat{r} does not hold on interval k . Thus, \hat{r} does not hold on interval k and T_c does not hold on interval k , due to the fact that we picked k so that $s_k(\llbracket \beta \rrbracket) = \text{true}$. By the fact that I_j is the last interval on which $\llbracket \alpha \mathbf{U}_{>n}^s \beta \rrbracket$ holds, we know that c and *righto* are set based on Constraint 14 on interval $j+1$ and based on Constraint 15 on all later intervals. This implies that at interval k , the value of $c + \delta$ is the difference between the right bounds of I_k

and I_j . Furthermore, $s_k(\text{righto}) = \text{true}$ iff I_j is open. Now

- If I_j is open, then by the fact that T_c does not hold on interval k we know that the difference between the right bounds of I_j and I_k is less than n . This, however, contradicts the fact that k was chosen such that for every point in I_j there is a point in I_k that is more than n time units away.
- If I_j is a singleton, then the difference between the right bounds of I_j and I_k is less than or equal to n . Again, this contradicts the fact that for every point in I_j there is a point in I_k that is more than n time units away.

Thus, assuming that the fairness constraint $\mathcal{F}_{\alpha \mathbf{U}_{>n}^s \beta}$ is not satisfied leads to a contradiction. ■

Proof: For $\mathbf{Op} = \mathbf{U}_{\geq n}^s$. To obtain the proof for $\mathbf{U}_{\geq n}^s$, we make the following changes to the proof for $\mathbf{U}_{>n}^s$.

- All cases in which $n = 0$ are now contradictions, as we encode $\mathbf{U}_{\geq 0}^s$ by the \mathbf{U}^s encoding.
- No substantial changes are needed to show that Constraints 10 and 11 are satisfied.
- When showing that Constraints 12 and 13 are satisfied:
 - In the case where $s_i(\text{oblig}) = s_i(\llbracket \alpha \mathbf{U}_{\geq n}^s \beta \rrbracket) = \text{true}$ the only valid option is that $s_{i+1}(\text{oblig}) = s_{i+1}(\llbracket \alpha \rrbracket) = \text{true}$, as all other cases required $n = 0$.
 - In the case where $s_i(\text{oblig}) = \text{true}$ and $s_i(\llbracket \alpha \mathbf{U}_{\geq n}^s \beta \rrbracket) = \text{false}$, we pick k so that for every point in j there is a point at least n time units away in I_k (and the properties regarding $\llbracket \alpha \rrbracket$ and $\llbracket \beta \rrbracket$ hold). After picking m , we note that if T_c does not hold on interval m then by the definition of T_c the difference between the right bounds of I_m and I_j is less than or equal to n and less than n if I_j is open or I_m is a singleton. Then, there is a point in I_j for which there is no point in I_m that is $\geq n$ time units away. Again, we conclude that $k \neq m$. We proceed as before.
- When showing that the fairness constraint is satisfied we pick k so that for every point in j there is a point at least n time units away in I_k (and the properties regarding $\llbracket \alpha \rrbracket$ and $\llbracket \beta \rrbracket$ hold).

Then, the final case distinction is replaced by

- If I_j is open or I_k a singleton, then by the fact that T_c does not hold on interval k we know that the difference between the right bounds of I_j and I_k is less than n . This, however, contradicts the fact that k was chosen such that for every point in I_j there is a point in I_k that is at least n time units away.
- If I_j is a singleton and I_k an open interval, then the difference between the right bounds of I_j and

I_k is less than or equal to n . Again, this contradicts the fact that for every point in I_j there is a point in I_k that is at least n time units away. ■

Proof: For $\mathbf{Op} = \mathbf{R}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) / s_i(\llbracket \alpha \rrbracket) / s_i(\llbracket \beta \rrbracket)$ to **true** iff $\sigma^{(i, \cdot)} \models \alpha \mathbf{R}^s \beta / \sigma^{(i, \cdot)} \models \alpha / \sigma^{(i, \cdot)} \models \beta$, respectively. We set $s_i(\text{oblig}) = \text{true}$ iff at least one of the following holds:

- 1) I_i is open and $s_i(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$,
- 2) I_{i-1} is a singleton and $s_{i-1}(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$, or
- 3) $s_{i-1}(\text{oblig}) = \text{true}$ and $s_{i-1}(\llbracket \alpha \rrbracket) = \text{false}$.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. Constraints 16, 17 and 18 are trivially satisfied based on the rules for setting the value of *oblig*. Thus, it only remains to be shown that Constraint 19 is satisfied as well. We distinguish the following cases:

- Case 1: $s_i(\text{oblig}) = \text{false}$. In this case, Constraint 19 is trivially satisfied.
- Case 2: $s_i(\text{oblig}) = \text{true}$ and Rule 1 for setting the value of *oblig* applies. That is, I_i is open and $s_i(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$. As $s_i(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$, we know that $\sigma^{(i, \cdot)} \models \alpha \mathbf{R}^s \beta$. On any open interval satisfying $\alpha \mathbf{R}^s \beta$ either α or β (or both) must hold, immediately implying that Constraint 19 is satisfied.
- Case 3: $s_i(\text{oblig}) = \text{true}$ and Rule 1 does not apply but Rule 2 does apply. Then I_{i-1} is a singleton and $s_{i-1}(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$, implying that $\sigma^{(i-1, \cdot)} \models \alpha \mathbf{R}^s \beta$. If I_i itself is a singleton, then there is no time point in between the single time point in I_{i-1} and the single time point in I_i . Thus, $\sigma^{(i-1, \cdot)} \models \alpha \mathbf{R}^s \beta$ implies that $s_i(\llbracket \beta \rrbracket) = \text{true}$, in turn implying that Constraint 19 is satisfied. If, in contrast, I_i is open, then $\sigma^{(i-1, \cdot)} \models \alpha \mathbf{R}^s \beta$ implies that either $s_i(\llbracket \alpha \rrbracket) = \text{true}$ or $s_i(\llbracket \beta \rrbracket) = \text{true}$ (or both). Thus, also in this case Constraint 19 is satisfied.
- Case 4: $s_i(\text{oblig}) = \text{true}$ and Rule 1 and Rule 2 do not apply. In this case, Rule 3 has to apply, as we would not have set $s_i(\text{oblig}) = \text{true}$ if no rule applied. Thus, $s_{i-1}(\text{oblig}) = \text{true}$ and $s_{i-1}(\llbracket \alpha \rrbracket) = \text{false}$. We now choose $j < i$ as large as possible such that (i) $s_j(\text{oblig}) = \text{true}$ and (ii) either $j = 0$ or $s_{j-1}(\text{oblig}) = \text{false}$. Now we know that $s_j(\text{oblig}) = \text{true}$ based on Rule 1 or Rule 2. Let $\bar{j} = j$ iff Rule 1 applies to interval j and $\bar{j} = j - 1$ otherwise. We now know that $s_{\bar{j}}(\llbracket \alpha \mathbf{R}^s \beta \rrbracket) = \text{true}$ and, thus, $\sigma^{(\bar{j}, \cdot)} \models \alpha \mathbf{R}^s \beta$. Furthermore, as *oblig* propagated up to interval i through Rule 3, we know that $s_j(\llbracket \alpha \rrbracket) = \dots = s_{i-1}(\llbracket \alpha \rrbracket) = \text{false}$. Now take any $t_1 \in I_i$ and $t_2 \in I_j$. We now perform another case distinction based on the type of I_i .
 - If I_i is a singleton, then for any $(k, t) \in T(\sigma)$ with $(\bar{j}, t_2) \prec (k, t) \prec (i, t_1)$ it holds that $j \leq k < i$,

implying that $s_k(\llbracket \alpha \rrbracket) = \text{false}$. Thus, there is no time point in between (\bar{j}, t_2) and (i, t_1) at which α holds. As $\sigma^{(\bar{j}, t_2)} \models \alpha \mathbf{R}^s \beta$, this means that $s_i(\llbracket \beta \rrbracket) = \text{true}$ and Constraint 19 is satisfied.

- If I_i is open, then for any $(k, t) \in T(\sigma)$ with $(\bar{j}, t_2) \prec (k, t) \prec (i, t_1)$ it holds that $j \leq k \leq i$, meaning that $s_j(\llbracket \alpha \rrbracket) = \text{true}$ implies $k = i$. Thus, if there is a time point in between (\bar{j}, t_2) and (i, t_1) at which α holds, that time point has to be part of interval i , meaning that $s_i(\llbracket \alpha \rrbracket) = \text{true}$. If there is no such time point, then the fact that $\sigma^{(\bar{j}, t_2)} \models \alpha \mathbf{R}^s \beta$ implies that $s_i(\llbracket \beta \rrbracket) = \text{true}$. Hence, we have $s_i(\llbracket \alpha \rrbracket) = \text{true}$ or $s_i(\llbracket \beta \rrbracket) = \text{true}$ (or both) and Constraint 19 is satisfied.

Either way, we were able to demonstrate that Constraint 19 is satisfied. ■

Proof: For $\mathbf{Op} = \mathbf{G}_{\leq 0}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) / s_i(\llbracket \alpha \rrbracket)$ to **true** iff $\sigma^{(i, \cdot)} \models \mathbf{G}_{\leq 0}^s \alpha / \sigma^{(i, \cdot)} \models \alpha$, respectively.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. Now

- If $s_i(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \text{false}$ or I_i is open or I_{i+1} is open, then Constraint 20 is trivially satisfied on interval i .
- If, $s_i(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \text{true}$ and I_i is a singleton and I_{i+1} is a singleton, then pick $j \geq i + 1$ as large as possible such that I_i, \dots, I_j are all singletons. $s_i(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \text{true}$ means that $\sigma^{(i, \cdot)} \models \mathbf{G}_{\leq 0}^s \alpha$. Thus, we know that $s_{i+1}(\llbracket \alpha \rrbracket) = \dots = s_j(\llbracket \alpha \rrbracket) = \text{true}$. This implies that $\sigma^{(i+1, \cdot)} \models \llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket$ as well and, thus, $s_{i+1}(\llbracket \mathbf{G}_{\leq 0}^s \alpha \rrbracket) = \text{true}$. Thus, Constraint 20 is satisfied on interval i in this case as well.

Hence, Constraint 20 is in each case satisfied on interval i . ■

Proof: For $\mathbf{Op} = \mathbf{G}_{< n}^s$. Auxiliary variable rules: Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \mathbf{G}_{< n}^s \alpha \rrbracket) / s_i(\llbracket \alpha \rrbracket)$ to **true** iff $\sigma^{(i, \cdot)} \models \mathbf{G}_{< n}^s \alpha / \sigma^{(i, \cdot)} \models \alpha$, respectively. We set $s_0(c) = n + 1$ and $s_0(\text{righto}) = \text{true}$. For $i > 0$ we set $s_i(c)$ and $s_i(\text{righto})$ according to Constraints 22 and 23 and s_{i-1} .

The transition constraints are satisfied: Let $i \in \mathbb{N}$.

It remains to show that Constraint 21 is satisfied on interval i .

- Case 1: T_c does not hold on interval i and $s_i(\llbracket \mathbf{G}_{< n}^s \alpha \rrbracket) = \text{false}$ or I_i is a singleton. In this case Constraint 21 is trivially satisfied.
- Case 2: $s_i(\llbracket \mathbf{G}_{< n}^s \alpha \rrbracket) = \text{true}$ and I_i is open. As $\sigma^{(i, \cdot)} \models \mathbf{G}_{< n}^s \alpha$ and I_i is open, we now know that $s_i(\llbracket \alpha \rrbracket) = \text{true}$. Thus, Constraint 21 is satisfied.
- Case 3: T_c holds on interval i . Then we note that there is a previous interval on which $\llbracket \mathbf{G}_{< n}^s \alpha \rrbracket$ holds. If no such previous interval would exist, then $s_i(c)$ would be at least the initial value of $n + 1$, contradicting the assumption that T_c holds. We can, thus, pick $j < i$ as large as possible such that $s_j(\llbracket \mathbf{G}_{< n}^s \alpha \rrbracket) = \text{true}$, implying $\sigma^{(j, \cdot)} \models \mathbf{G}_{< n}^s \alpha$.

As is easy to see, repeated application of Constraints 22 and 23 leads to $s_i(c)$ being the difference between the left bound of I_i and the right bound of I_j . Furthermore, $s_i(righto) = \text{true}$ iff I_j is open. As T_c holds at interval i we know that $s_i(c) < n$. That is, the difference between left bound of I_i and the right bound of I_j is less than n time units. Indiscriminately of whether I_j and I_i are open or singletons, this implies that there are $t_1 \in I_i$ and $t_2 \in I_j$ with $t_1 - t_2 < n$. This implies that $s_i(\llbracket \alpha \rrbracket) = \text{true}$, as $\sigma^{(j,\cdot)} \models \mathbf{G}^s_{<n} \alpha$. Thus, Constraint 21 is satisfied in this case as well. ■

Proof: For $\mathbf{Op} = \mathbf{G}^s_{\leq n}$. The proof for $\mathbf{Op} = \mathbf{G}^s_{\leq n}$ proceeds precisely as the proof for $\mathbf{Op} = \mathbf{G}^s_{<n}$ up to the point in Case 2 where we observe that $s_i(c) < n$. For $\mathbf{Op} = \mathbf{G}^s_{\leq n}$, we observe instead that $s_i(c) < n$ or $s_i(c) \leq n$ and intervals I_i and I_j are both singletons. Thus, we can pick time points in I_i and I_j that are $\leq n$ time units apart. Hence, the fact that $\sigma^{(j,\cdot)} \models \mathbf{G}^s_{<n} \alpha$ again implies $s_i(\llbracket \alpha \rrbracket) = \text{true}$ and Constraint 21 is satisfied. ■

Proof: For $\mathbf{Op} = \mathbf{R}^s_{>n}$. **Auxiliary variable rules:** Let $i \in \mathbb{N}$. As always, we set $s_i(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) / s_i(\llbracket \alpha \rrbracket) / s_i(\llbracket \beta \rrbracket)$ to **true** iff $\sigma^{(i,\cdot)} \models \alpha \mathbf{R}^s_{>n} \beta / \sigma^{(i,\cdot)} \models \alpha / \sigma^{(i,\cdot)} \models \beta$, respectively. We set $s_0(c) = 0$ and $s_0(lefto) = \text{false}$. For $i > 0$ we set $s_i(c)$ and $s_i(lefto)$ according to Constraints 29, 30 and 31 and s_{i-1} . For setting the value of *oblig*, we use the same rules used for the untimed release \mathbf{R}^s . That is, we set $s_i(\text{oblig}) = \text{true}$ iff at least one of the following holds:

- 1) I_i is open and $s_i(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$,
- 2) I_{i-1} is a singleton and $s_{i-1}(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$, or
- 3) $s_{i-1}(\text{oblig}) = \text{true}$ and $s_{i-1}(\llbracket \alpha \rrbracket) = \text{false}$.

The initial constraint is satisfied: Initial Constraint $\mathcal{I}_{\alpha \mathbf{R}^s_{>n} \beta}$ is trivially satisfied as $s_0(c) = 0$ and $s_0(lefto) = \text{false}$.

The transition constraints are satisfied: Let $i \in \mathbb{N}$. We observe that Constraints 24, 25 and 26 correspond to Constraints 16, 17 and 18 in the encoding of the untimed release operator. Consequently, Constraints 24, 25 and 26 are satisfied by the fact that we use the exact same rules for setting the value of $s_i(\text{oblig})$.

The left hand side of the implication in Constraint 28 is satisfied precisely if $\sigma^{(i,\cdot)} \models \alpha \mathbf{R}^s_{>n} \beta$ and I_i is an open interval whose bounds are more than n time units apart. Then, there are time points $t_1, t_2 \in I_i$ such that $t_2 - t_1 > n$. By the semantics of \mathbf{R}^s , this implies that β holds at (i, t_2) or that α holds somewhere in between (i, t_1) and (i, t_2) . Thus, $s_i(\llbracket \alpha \rrbracket) = \text{true}$ or $s_i(\llbracket \beta \rrbracket) = \text{true}$ and the right hand side of the implication is satisfied as well.

We now argue that Constraint 27 is satisfied on interval i using a case distinction:

Case 1: $s_i(\text{oblig}) = \text{false}$ or T_c is not satisfied at interval i or interval I_i is open and $s_i(\llbracket \alpha \rrbracket) = \text{true}$. In this case, Constraint 27 is trivially satisfied at interval i .

Case 2: $s_i(\text{oblig}) = \text{true}$, either I_i is a singleton or $s_i(\llbracket \alpha \rrbracket) = \text{false}$ and T_c is satisfied at interval i . Note that T_c holding at interval i implies that $s_i(c) > 0$. Now pick $j \leq i$ as large as possible such that one of the following: (i) $j < i$ and D_c holds at interval j , (ii) R_c holds at interval $j - 1$ or (iii) $j = 0$. By the choice of j we know that (a) R_c does not hold at intervals $j \dots i - 1$ (b) D_c does not hold at intervals $j + 1, \dots, i - 1$ and (c) $s_j(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$. If j was chosen based on (i) or (ii), this immediately follows from the definition of D_c and R_c . If, in contrast, j was chosen based on (iii) (implying $j = 0$) then assuming $s_j(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{false}$ leads to the observation that both $\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket$ and *oblig* are **false** on a prefix of τ . Thus R_c holds on the first interval on whose successor $\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket$ holds. As $s_i(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$, this the case on is interval $i - 1$ at the latest, contradicting the assumption that we picked j based on (iii). Thus, $s_j(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$ in each case.

Based on the update rules for c and *lefto*, we know that $s_i(\text{lefto}) = \text{true}$ iff I_j is open. Furthermore, $s_i(c)$ is the difference between the left bound of I_i and the left bound of I_j , i.e. $s_i(c) + s_i(\delta)$ is the difference of the right bound of I_i and the left bound of I_j . By our Case 2 assumption that T_c is satisfied, this difference is greater than n . Therefore, we can indiscriminately of the type of I_i and I_j pick $t_1 \in I_i, t_2 \in I_j$ such that $t_1 - t_2 > n$.

Let $\bar{i} := i$ if I_i is open and $\bar{i} := i - 1$ otherwise. Furthermore, let $\bar{j} := j$ if I_j is open and $\bar{j} := j + 1$ otherwise. Note that $\bar{i} \geq \bar{j}$. (As $i > j$, we know that $\bar{i} \geq \bar{j} - 1$. Additionally, $\bar{i} = \bar{j} - 1$ would require that $i = j + 1$ and that both I_i and I_j to be singletons which contradicts $c + \delta > n$ at interval i) Furthermore, note that the time points lying in between (j, t_1) and (i, t_2) now all belong to $I_{\bar{j}}, \dots, I_{\bar{i}}$. We now claim that both $s_{\bar{j}}(\text{oblig}) = \dots = s_{\bar{i}}(\text{oblig}) = \text{true}$ and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{\bar{i}}(\llbracket \alpha \rrbracket) = \text{false}$. Note, that by our Case 2 assumptions we have $s_i(\text{oblig}) = \text{true}$ and $s_i(\llbracket \alpha \rrbracket) = \text{false}$ if I_i is open (meaning $\bar{i} = i$). Thus, we only have to show that $s_{\bar{j}}(\text{oblig}) = \dots = s_{i-1}(\text{oblig}) = \text{true}$ and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{i-1}(\llbracket \alpha \rrbracket) = \text{false}$, which will proven by induction over $k = \bar{j}, \dots, i - 1$, for each k assuming that we established $s_{\bar{j}}(\text{oblig}) = \dots = s_{k-1}(\text{oblig}) = \text{true}$ and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{k-1}(\llbracket \alpha \rrbracket) = \text{false}$ already.

Base case: $k = \bar{j}$. $s_{\bar{j}}(\text{oblig}) = \text{true}$ follows immediately from the fact that $s_j(\llbracket \alpha \mathbf{R}^s_{>n} \beta \rrbracket) = \text{true}$ and Rules 1 and 2 for setting the value of *oblig*.

Now assume $s_k(\llbracket \alpha \rrbracket) = \text{true}$. Recall, that $s_i(\text{oblig}) = \text{true}$. This allows us to pick a m as small as possible such that $k < m \leq i$ and $s_m(\text{oblig}) = \text{true}$. Then:

- If $m = k + 1$, then based on the fact that $s_k(\llbracket \alpha \rrbracket) = \text{true}$, we know that *oblig* was set to **true** on interval m not based on Rule 3 but based on Rule 1 or 2.
- If $m > k + 1$, then by the choice of m we know that $s_{m-1}(\text{oblig}) = \text{false}$. Thus, we deduct that, again, *oblig* was not set to **true** on interval m based on Rule 3 but based on Rule 1 or 2.

Now we split based on the rule by which *oblig* was set to **true** on interval m .

- If *oblig* was set to **true** based on Rule 1 and Rule 2 does not apply, then $s_m(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$ and $s_{m-1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{false}$ (as otherwise Rule 2 would apply). Furthermore, I_m is open, implying that I_{m-1} is asingleton.
 - If $m = k + 1$, then as $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$, $s_k(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{false}$ and $s_{k+1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$ we conclude that R_c holds at interval $m-1 = k > j$, contradicting observation (a).
 - If $m > k + 1$, then $s_{m-1}(\mathit{oblig}) = \mathbf{false}$. As additionally $s_m(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$, $s_k(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{false}$, we know that R_c holds on interval $m-1 > k \geq j$, again contradicting observation (a).
- If *oblig* was set to **true** based on Rule 2, then I_{m-1} is a singleton and $s_{m-1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$. Now:
 - If $m = k + 1$, then I_k is a singleton, implying that $k > j$ (as $k \geq \bar{j}$ it is not possible that $k = j$ when I_k is a singleton). Now $s_k(\llbracket \alpha \rrbracket) = s_k(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = s_k(\mathit{oblig}) = \mathbf{true}$, I_k is a singleton and D_c holds at interval $k > j$. This contradicts observation (b).
 - If $m = k + 2$, we further split cases based on the type of I_k .
 - * If I_k is open, then $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$ and $s_{k+1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$, meaning that R_c is satisfied at interval k , again contradicting (a).
 - * If I_k is a singleton, then we again observe that $k > j$. Now one last split is necessary:
 - If $s_k(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$, then D_c holds at interval $k > j$, contradicting (b).
 - If $s_k(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{false}$, then R_c holds on interval k based on the fact that, additionally, $s_k(\llbracket \alpha \rrbracket) = \mathbf{true}$ and $s_{k+1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$, contradicting (a).
 - Assume $m > k + 2$. By the choice of m we know that $s_{m-2}(\mathit{oblig}) = \mathbf{false}$ and $s_{m-1}(\mathit{oblig}) = \mathbf{false}$, implying that $s_{m-2}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{false}$. Now R_c holds at interval $m-2 > k \geq j$ due to the fact that additionally $s_{m-1}(\llbracket \alpha \mathbf{R}_{>n}^s \beta \rrbracket) = \mathbf{true}$, again contradicting (a).

As each case ended in a contradiction we conclude that $s_k(\llbracket \alpha \rrbracket) = \mathbf{false}$.

Inductive step: $\bar{j} < k < i$. Now $s_k(\mathit{oblig}) = \mathbf{true}$ follows from the inductive hypothesis that $s_{k-1}(\mathit{oblig}) = \mathbf{true}$ and $s_{k-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$ and Rule 3 for setting the value of *oblig*. Furthermore, we can derive that $s_k(\llbracket \alpha \rrbracket) = \mathbf{false}$ by the same arguments used in the base case. Thus, we have shown inductively that $s_{\bar{j}}(\mathit{oblig}) = \dots = s_{i-1}(\mathit{oblig}) = \mathbf{true}$ and $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_{i-1}(\llbracket \alpha \rrbracket) = \mathbf{false}$.

Now as $s_{\bar{j}}(\llbracket \alpha \rrbracket) = \dots = s_i(\llbracket \alpha \rrbracket) = \mathbf{false}$ we know that there is no time point in between (j, t_2) and (i, t_1) at which α holds. As $\sigma^{(j, t_2)} \models \alpha \mathbf{R}_{>n}^s \beta$ and $t_1 - t_2 > n$ we can conclude that β holds at time point (i, t_1) , meaning that $s_i(\llbracket \beta \rrbracket) = \mathbf{true}$ and ultimately implying that Constraint 27 is satisfied at interval i . ■

Proof: For $\mathbf{Op} = \mathbf{R}_{\geq n}^s$. To adapt the proof for $\mathbf{Op} = \mathbf{R}_{>n}^s$ to $\mathbf{Op} = \mathbf{R}_{\geq n}^s$ we only need to argue that in Case 2, based on the fact that T_c holds we can pick $t_1 \in I_i$, $t_2 \in I_j$ with $t_1 - t_2 \geq n$. As T_c holds, we know that the difference between the right bound of I_i and the left bound of I_j is $> n$ or the difference is $\geq n$ and both I_i and I_j are singletons. In both cases, we can pick t_1, t_2 with $t_1 - t_2 \geq n$. ■

G. Proof of Lemma 6

Lemma 6: Assume two states, s and t , such that $s \approx t$. It holds that (i) $s \models \mathcal{I}$ iff $t \models \mathcal{I}$, and (ii) $s \models \mathcal{INV}$ iff $t \models \mathcal{INV}$. Furthermore, if there is a $\delta_s \in \mathbb{R}_{\geq 0}$ and a state s' such that $s \cup \{\delta \mapsto \delta_s\} \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\} \models \mathcal{T}$, then there is a $\delta_t \in \mathbb{R}_{\geq 0}$ and a state t' such that $t \cup \{\delta \mapsto \delta_t\} \cup \{y' \mapsto t'(y) \mid y \in X \cup Z\} \models \mathcal{T}$ and $s' \approx t'$.

Proof: As $s \approx t$ and the only atoms involving clock variables in \mathcal{I} and \mathcal{INV} are of form $x \bowtie n$, the definitions of m_x and \approx directly imply that (i) $s \models \mathcal{I}$ iff $t \models \mathcal{I}$, and (ii) $s \models \mathcal{INV}$ iff $t \models \mathcal{INV}$.

To prove the remaining claim, consider the state s'' such that (i) $s''(x) = s(x) + \delta_s$ for each clock $x \in X$, and (ii) $s''(z) = s'(z)$ for each non-clock $z \in Z$. As $s \cup \{\delta \mapsto \delta_s\} \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\} \models \mathcal{T}$, we have $\delta_s \geq 0$ and for each $x \in X$ either $s'(x) = 0$ or $s'(x) = s(x) + \delta_s = s''(x)$. That is, intuitively s'' is obtained from s' by “unresetting” the reset clocks.

Next, take any $\delta_t \in \mathbb{R}$ and state t'' such that (i) $\delta_t \geq 0$, (ii) $\delta_t = 0 \Leftrightarrow \delta_s = 0$, (iii) $t''(x) = t(x) + \delta_t$ for each clock $x \in X$, (iv) $t''(z) = s'(z)$ for each non-clock $z \in Z$, and (v) $s'' \approx t''$. Such δ_t and t'' exists because $s \approx t$ and of the fact that clock valuations in the same region have time successors in same regions [1]. Let t' be the state such that (i) for each $x \in X$, $t'(x) = 0$ if $s'(x) = 0$ and $t'(x) = t''(x) = t(x) + \delta_t$ otherwise, and (ii) $t'(z) = t''(z) = s'(z)$ for each non-clock $z \in Z$. Now $s' \approx t'$. As a summary, intuitively t' is a state in the region that is obtained by letting time pass in the similar manner as when moving from s to s' and then resetting the same clocks.

Now we only have to show that $t \cup \{\delta \mapsto \delta_t\} \cup \{y' \mapsto t'(y) \mid y \in X \cup Z\} \models \mathcal{T}$. We do this by showing that the atoms in \mathcal{T} evaluate to the same boolean value under both $s \cup \{\delta \mapsto \delta_s\} \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\}$ and $t \cup \{\delta \mapsto \delta_t\} \cup \{y' \mapsto t'(y) \mid y \in X \cup Z\}$.

- Case: the atom does not involve variables in $X \cup X' \cup \{\delta\}$.

In this case the atom evaluates to true under $s \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\}$ if and only if it does under $t \cup \{y' \mapsto t'(y) \mid y \in X \cup Z\}$ because $s \approx t$ and $s' \approx t'$.

- Case: the atom is of form $x' = 0$.
Because $s' \approx t'$, the atom evaluates to true under $\{y' \mapsto s'(y) \mid y \in X \cup Z\}$ if and only if it does under $\{y' \mapsto t'(y) \mid y \in X \cup Z\}$.
- Case: the atom is of form $x' = x + \delta$.

We have to consider the following:

- 1) Sub-case $s'(x) = 0$.

Thus $t'(x) = 0$ as well because $s' \approx t'$. Now $x' = x + \delta$ evaluates to true under $s \cup \{\delta \mapsto \delta_s\} \cup \{y' \mapsto s'(y) \mid y \in X \cup Z\}$ if and only if $s(x) = 0$ and $\delta_s = 0$ (as x and δ always have non-negative values).

- a) If $s(x) = 0$ and $\delta_s = 0$, then $t(x) = 0$ and $\delta_t = 0$ as well because $s \approx t$ and $s'' \approx t''$ (forcing that $s(x) + \delta_s = 0$ if and only if $t(x) + \delta_t = 0$).
- b) If $s(x) > 0$, then $t(x) > 0$ as $s \approx t$, and thus $s'(x) \neq s(x) + \delta_s$ and $t'(x) \neq t(x) + \delta_t$.
- c) If $s(x) = 0$ and $\delta_s > 0$, then $t(x) = 0$ as

$s \approx t$ and $\delta_t > 0$ as $s'' \approx t''$ and $s''(x) = s(x) + \delta_s \geq 0$, implying that $s'(x) \neq s(x) + \delta_s$ and $t'(x) \neq t(x) + \delta_t$.

- 2) Sub-case $s'(x) > 0$.

Now also $t'(x) > 0$ as $s' \approx t'$. As $s'(x) > 0$, it must be that $s'(x) = s(x) + \delta_s$ of the restriction imposed on \mathcal{T} . By the construction of t'' and t' , $t'(x) = t''(x) = t(x) + \delta_t$.

- Case: the atom is of form $x \bowtie n$.
Because $s \approx t$, the atom evaluates to true under s if and only if it does under t .
- Case: the atom is of form $x + \delta \bowtie n$.
By the construction of s'' and t'' , and the fact that $s'' \approx t''$, we have that $s''(x) = s(x) + \delta_s \bowtie n$ if and only if $t''(x) = t(x) + \delta_t \bowtie n$.
- Case: the atom is of form $\delta \bowtie 0$.
Because $\delta_s \geq 0$, $\delta_t \geq 0$, and $\delta_s = 0 \Leftrightarrow \delta_t = 0$, the atom evaluates to true under $\{\delta \mapsto \delta_s\}$ if and only if it does under $\{\delta \mapsto \delta_t\}$.

■